Satyrn INDUSTRIAL SWITCHES

SATYRN X SERIES

USER MANUAL

Comtrol GmbH | Unit 2 | Staplehurst |Weston on the Green

Bicester | OX25 3QU | UK

+44 1869 352740

www.comtrol.co.uk

Table of Content

1 Getting to Know Your Switch 1
1.1 About the X Series Industrial Switch 1
1.2 Software Features 1
1.3 Hardware Features 2
2 Hardware installation 2
3 Layout 3
3.1 Satyrn X244-GQ/X244-GQ-P 3
3.1.1 General 3
3.1.2 Front View 3
3.1.3 Rear View 3
3.2 Satyrn X244-TQ 4
3.2.1 Front View 4
3.2.2 Rear View 4
3.3 Satyrn X168-CQ 4
3.3.1 Front View 5
3.3.2 Rear View 5
4 Cables 5
4.1 Ethernet Cables 5
4.1.1 100BASE-TX/10BASE-T RJ-45 Pin assignments 6
4.1.2 1000 Base T Pin RJ-45 assignments 6
4.1.3 MDI/MD-X operation 6
4.2 SFP 7
4.3 Console Cable 8

5 Configuring the switch 8
5.1 Configuring the X Series Satyrn switches using a Browser 8
5.2 Satyrn View 9
5.3 Switch Function Interface 9
5.4 Command Line Interface 10
6 Browser and Satyrn View's Switch Function Interface 10
6.1 System Information 10
6.1.1 Location Alert 10
6.2 Basic Setting 11
6.2.1 Basic Settings 11
6.2.2 Admin Password 11
6.2.3 IP Setting 12
6.2.4 IPv6 Setting 13
6.2.5 HTTPS 14
6.2.6 SSH 14
6.2.7 LLDP 14
6.2.7.1 LLDP Configuration 15
6.2.7.2 LLDP Neighbour Information 16
6.2.7.3 LLDP Statistics 17
6.2.8 Backup/Restore Configuration 18
6.2.9 Upgrade Firmware 18
6.3 DHCP Server 19
6.3.1 Setting 19
6.3.2 DHCP Dynamic Client List 20
6.3.3 DHCP Static Client 20

6.4 Port Setting 20
6.4.1 Port Configuration 21
6.4.2 Rate Limit 22
6.4.3 Port Trunk 23
6.4.3.1 LACP Port Configuration 24
6.4.3.2 LACP System Status 25
6.4.3.3 LACP Status 26
6.4.3.4 LACP Statistics 27
6.4.4 Loop Guard 28
6.5 Redundancy 28
6.5.1 Satyrn-Ring 28
6.5.2 Satyrn Link 30
6.5.3 MSTP 30
6.5.3.1 Bridge settings 30
6.5.3.2 MSTI mapping 32
6.5.3.3 MSTI priorities 33
6.5.3.4 CIST ports 34
6.5.3.5 MSTI ports 35
6.5.3.6 Bridge Status 37
6.5.3.7 STP Port Status 38
6.5.3.8 STP Statistics 38
6.5.4 Fast Recovery 39
6.6 VLAN 40
6.6.1 VLAN Membership Configuration 40
6.6.2 VLAN Port 40

6.6.3 Private VLAN 42
6.6.3.1 Membership 42
6.6.3.2 Port Isolation 43
6.7 SNMP 43
6.7.1 SNMP-Configuration 43
6.7.1.1 SNMP-System configuration 43
6.7.1.2 SNMP Trap configuration 45
6.7.2 SNMP-Communities 46
6.7.3 SNMP-Users 47
6.7.4 SNMP-Groups 49
6.7.5 SNMP-Views 49
6.7.6 SNMP-Accesses 50
6.8 Traffic Prioritization 51
6.8.1 Storm Control 51
6.8.2 Port QoS Configuration 52
6.8.3 QoS Control List Configuration 53
6.8.4 Queuing Counters 55
6.8.5 Wizard 56
6.9 Multicast 57
6.9.1 IGMP Snooping 57
6.9.1.1 IGMP Configuration 57
6.9.2 IGMP Snooping Status 58
6.10 Security 59
6.10.1 ACL 59
6.10.1.1 ACL port configuration 59

6.10.1.2 ACL Rate Limiter 61
6.10.1.3 Access Control List Configuration 61
6.10.1.4 ACL Wizard 63
6.10.2 802.1x 64
6.10.2.1 Configuration 65
6.10.2.2 Port Security Status 67
6.10.2.3 802.1x Statistics 68
6.10.2.4 Authentication 71
6.10.2.5 RADIUS Authentication and Accounting Server Status 73
6.10.2.6 RADIUS Statistics 74
6.11 Warning 78
6.11.1 Satyrn Warning 78
6.11.2 System Warning ..... **Error! Bookmark not defined.**
6.12 Monitor and Diagnostics 81
6.12.1 MAC Table 81
6.12.1.1 MAC Table Configuration 81
6.12.1.2 MAC Address Table 82
6.12.2 Port Statistics 84
6.12.2.1 Port Traffic Overview 84
6.12.2.2 Detail Port Statistics 84
6.12.3 Port Monitoring (Mirroring) 86
6.12.4 System Log 87
6.12.5 Cable Diagnostics 88
6.12.6 ICMP & ICMPv6 Ping 89
6.13 Power over Ethernet 90

6.13.1 PoE Configuration 90
6.13.2 PoE Status 92
6.13.3 LLDP Neighbour Information 92
6.13.4 PoE Schedule 93
6.13.5 Auto Ping Check 94
6.14 Factory Defaults 95
6.15 System Reboot 96
7 Command Line Interface Management 97
7.1 About CLI Management 97
7.1.1 CLI Management by RS-232 Serial Console (115200, 8, none, 1, none) 97
7.1.2 CLI Management by Telnet 99
7.2 Commander Groups 101
7.2.1 System 101
7.2.2 Syslog 101
7.2.3 IP 102
7.2.4 Auth 102
7.2.5 Port 102
7.2.6 Aggr 103
7.2.7 LACP 103
7.2.8 STP 103
7.2.9 Dot1x 104
7.2.10 IGMP 105
7.2.11 LLDP 105
7.2.12 MAC 105
7.2.13 VLAN 106

7.2.14 PVLAN 106

7.2.15 QOS 106

7.2.16 ACL 107

7.2.17 Mirror 108

7.2.18 Config 108

7.2.19 SNMP 108

7.2.20 Firmware 109

7.2.21 Fault 109

Comtrol GmbH

Staplehurst

Weston on the Green

Bicester

OX25 3QU

UK

TELEPHONE

Switchboard	+44 (0) 1869 352740
Fax	+44 (0) 1869 351848
Support	+44 (0) 1869 352743

E-MAILS

Sales	sales@comtrol.co.uk
Support	support@comtrol.co.uk
Enquiries	enquiries@comtrol.co.uk
General	info@comtrol.co.uk

1 Getting to Know Your Switch

1.1 About the X Series Industrial Switch

The Satyrn X series switches are powerful 24-28 port managed redundant ring Gigabit Ethernet switches. With complete support of Ethernet Redundancy protocol, Satyrn Ring (recovery time < 20ms over 250 units of connection) and MSTP/RSTP/STP (IEEE 802.1s/w/D) these switches can protect your mission-critical applications from network interruptions or temporary malfunctions with their fast recovery technology.

The X series provides advanced IP-base bandwidth management which can limit the maximum bandwidth for each IP device. The user can prioritize IP cameras and NVR with more bandwidth while limiting the bandwidth of other devices. The X series switches also supports application based QoS which can prioritize data streams according to the TCP/UDP port number.

All functions of the X series switches can be managed centrally and conveniently by Satyrn View, Comtrol's powerful network management tool as well as via Web-based interface, Telnet and console (CLI) configurations. The switch is one of the most reliable choices for highly-managed and Gigabit Fibre Ethernet applications.

1.2 Software Features

- World's fastest Redundant Ethernet Ring (Recovery time < 10ms over 250 units connection)
- Supports Ring Coupling, Dual Homing, RSTP over Ring
- Supports SNMPv1/v2/v3 & RMON & Port base/802.1Q VLAN Network Management
- Event notification by Email, SNMP Trap and Relay Output
- Web-based ,Telnet, Console, and CLI configuration
- Enable/disable ports, MAC based port security
- Port based network access control (802.1x)
- VLAN (802.1q) to segregate and secure network traffic
- Radius centralized password management
- SNMPv3 encrypted authentication and access security
- RSTP (802.1w)
- Quality of Service (802.1p) for real-time traffic
- VLAN (802.1q) with double tagging and GVRP supported

- IGMP Snooping for multicast filtering
- Port configuration, status, statistics, mirroring, and security
- Remote Monitoring (RMON)

1.3 Hardware Features

- Redundant power inputs
- Operating Temperature: -40 to 70°C
- Storage Temperature: -40 to 85°C
- Operating Humidity: 5% to 95%, non-condensing
- Casing to IP 30
- X244-GQ – 24 Gigabit RJ45 ports + 4 Gigabit SFP ports, 110-240V AC
- X244-GQ-P – 24 Gigabit RJ45 ports + 4 Gigabit SFP ports, 110-240V AC + Dual 36-72VDC input
- X168-CQ – 16 Gigabit Combo ports + 4 Gigabit SFP ports, 110-240V AC
- X168-CQ-P – 16 Gigabit Combo ports + 4 Gigabit SFP ports, 110-240V AC + Dual 36-72VDC input
- X244-TQ – 24 Gigabit RJ45 ports (PoE+) + 4 Gigabit SFP ports, Triple 50-57VDC input
- X244-TQ-P – 24 Gigabit RJ45 ports (PoE+) + 4 Gigabit SFP ports, 110-240V AC with on-board 1000W power supply for PoE+
- Console Port
- 19-inch rack mountable

2 Hardware installation

The rack mount kit and screws are in the packing box. Please assembly the rack mount kit on the switch with the screws as shown below.

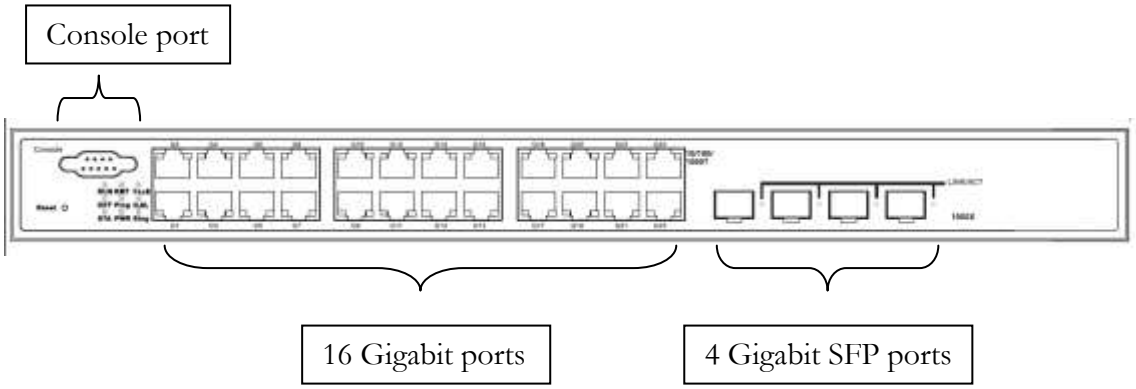
3 Layout

3.1 Satyrn X244-GQ/X244-GQ-P

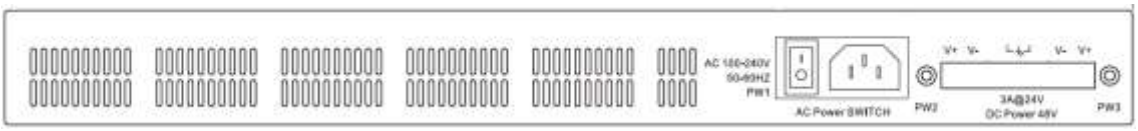
- X244-GQ – 24 Gigabit RJ45 ports + 4 Gigabit SFP ports, 110-240V AC
- X244-GQ-P – 24 Gigabit RJ45 ports + 4 Gigabit SFP ports, 110-240V AC + Dual 36-72VDC input

3.1.1 General

3.1.2 Front View



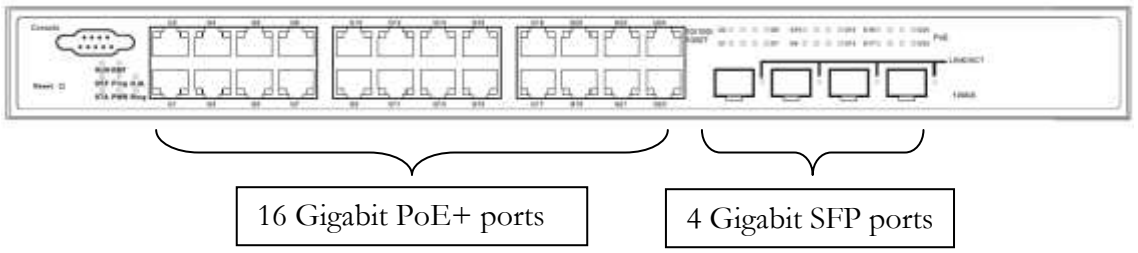
3.1.3 Rear View



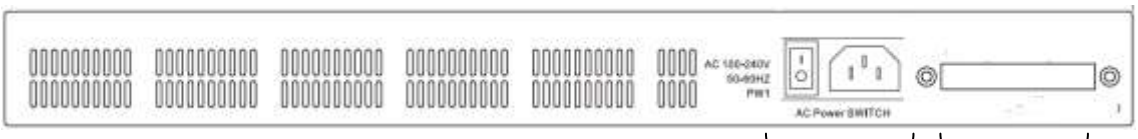
3.2 Satyrn X244-TQ

- X244-TQ – 24 Gigabit RJ45 ports (PoE+) + 4 Gigabit SFP ports, Triple 50-57VDC input
- X244-TQ-P – 24 Gigabit RJ45 ports (PoE+) + 4 Gigabit SFP ports, 110-240V AC with on-board 1000W power supply for PoE+

3.2.1 Front View



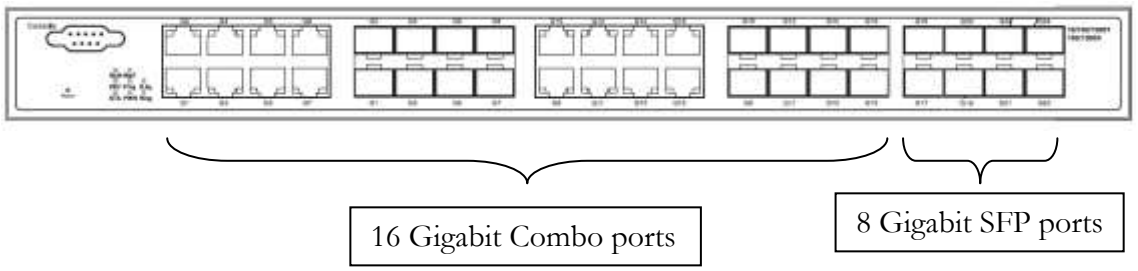
3.2.2 Rear View



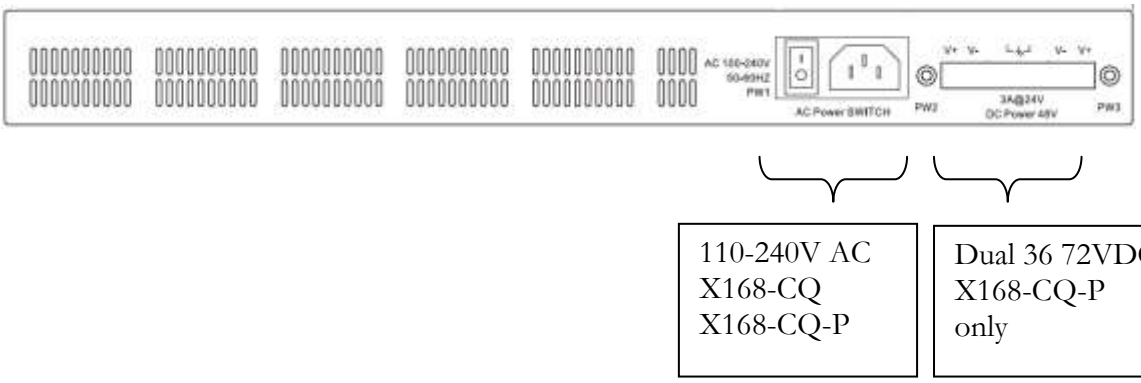
3.3 Satyrn X168-CQ

- X168-CQ – 16 Gigabit Combo ports + 4 Gigabit SFP ports, 110-240V AC
- X168-CQ-P – 16 Gigabit Combo ports + 4 Gigabit SFP ports, 110-240V AC + Dual 36-72VDC input

3.3.1 Front View



3.3.2 Rear View



4 Cables

4.1 Ethernet Cables

All of the X Series Satyrn switches have standard Ethernet ports. Depending on the link type, the switches use CAT 3, 4, 5,5e UTP cables to connect to any other network device. Please refer to the following table for cable specifications.

Cable	Type	Max. Length	Connector
10BASE-T	Cat. 3, 4, 5 100-ohm	UTP 100 m (328 ft)	RJ-45
100BASE-TX	Cat. 5 100-ohm UTP	UTP 100 m (328 ft)	RJ-45
1000Base-TX	Cat. 5/Cat. 5e 100-ohm UTP	100 m (328ft)	RJ-45

4.1.1 100BASE-TX/10BASE-T RJ-45 Pin assignments

With 100BASE-TX/10BASE-T cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 are used for receiving data.

Pin Number	Assignment
1	TD+
2	TD-
3	RD+
4	Not used (PoE + when available)
5	Not used (PoE + when available)
6	RD-
7	Not used (PoE - when available)
8	Not used (PoE - when available)

4.1.2 1000 Base T Pin RJ-45 assignments

With 1000 Base-T the RJ-45 Pin assignments are as follows

Pin Number	Assignment
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-

4.1.3 MDI/MD-X operation

The Satyrn X Series switches support auto MDI/MDI-X operation. You can use a straight-through cable to connect a PC to the switch. The following table shows the 10BASE-T/ 100BASE-TX MDI and MDI-X port pin outs.

10/100 Base-T MDI/MDI-X pins assignment

Pin Number	MDI port	MDI-X port
1	TD+(transmit)	RD+(receive)
2	TD-(transmit)	RD-(receive)
3	RD+(receive)	TD+(transmit)
4	Not used	Not used
5	Not used	Not used
6	RD-(receive)	TD-(transmit)
7	Not used	Not used
8	Not used	Not used

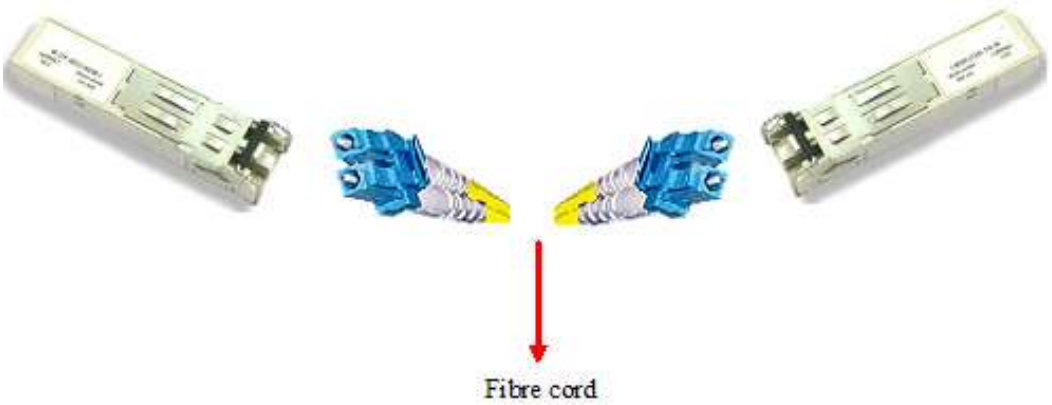
1000 Base-T MDI/MDI-X pins assignment

Pin Number	MDI port	MDI-X port
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

Note: "+" and "-" signs represent the polarity of the wires that make up each wire pair.

4.2 SFP

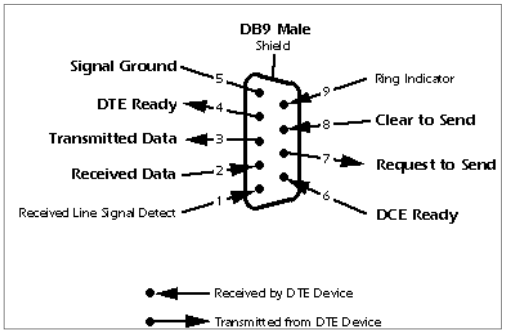
The X Series Switches have fibre optic ports with SFP adaptors with LC connector. Please remember that the TX port of Switch A should be connected to the RX port of Switch B.

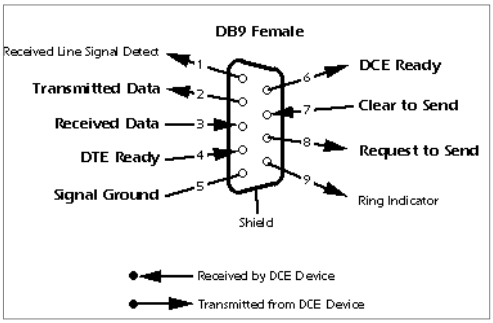


4.3 Console Cable

The X Series switches can be managed via a console port. The DB-9 to RJ-45 cable is found in the package. You can connect the switch to a PC via a RS-232 cable with DB-9 female connector while the other end (RJ-45 connector) connects to the console port on the switch.

PC pin out (male) assignment	RS-232 with DB9 female connector	DB9 to RJ 45
Pin #2 RD	Pin #2 TD	Pin #2
Pin #3 TD	Pin #3 RD	Pin #3
Pin #5 GD	Pin #5 GD	Pin #5





5 Configuring the switch

WARNING! – It is important that, whilst setting up or during firmware upgrade, you do NOT power off the switch.

There are a number of different ways to configure the X-Series switches. An inbuilt website can be used. Once coupled to Satyrn View Satyrn Explorer can be used and there is also a Command Line Interface (CLI) option.

This section applies to all of the X Series Satyrn switches. If there is additional information for specific models, this will be clearly stated.

5.1 Configuring the X Series Satyrn switches using a Browser

An embedded HTML web site resides in flash memory on the CPU board. It contains advanced management features and allows you to manage the switch from anywhere on the network through a standard web browser such as Microsoft Internet Explorer. The browser-based management function supports Internet Explorer 5.0 or higher. It is based on Java applets with an aim to reduce network bandwidth consumption, enhance access speed and provide an easy, useful interface.

Note: By default, version IE5.0 or later does not allow Java Applets to open sockets. You will need to explicitly modify the browser settings in order to enable Java applets to use the network port.

Preparing for Browser-based Management

The default settings are as follows:

IP Address	192.168.250.250
Subnet Mask	255.255.255.0
Default Gateway	192.168.250.1
User Name	comtrol
Password	satyrn

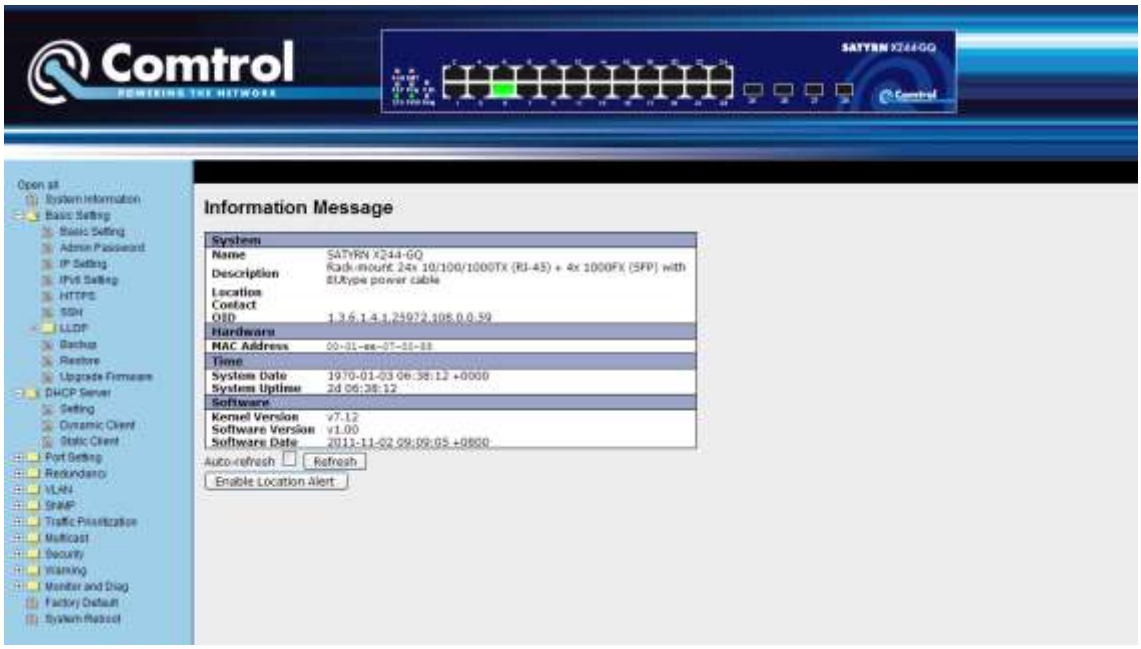
System Login

Launch Internet Explorer or another Internet browser.

Type http:// followed by the IP address of the switch (the default IP address is 192.168.250.250) into the address field and then press "Enter".

When the login screen appears, enter the User name and Password (the default User name is comtrol and the default Password is satyrn) into the fields and then press "Enter" or click the OK button.

The main interface of the Browser-based management will appear.

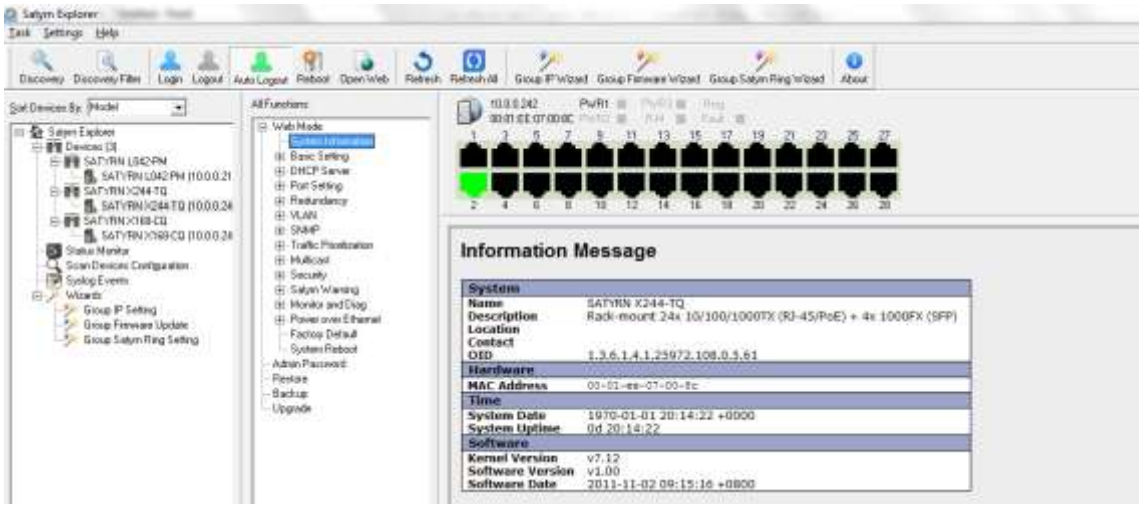


5.2 Satyrn View

Once the switches on the network have been identified (See Satyrn View 3.0 – Use Manual) using the Satyrn Explorer Interface and the switch has been selected, the Switch Function Interface appears.

5.3 Switch Function Interface

The switch function interface mirrors the Browser based Management available on the embedded firmware on the Switch.



Details in section 6 are identical for both interfaces.

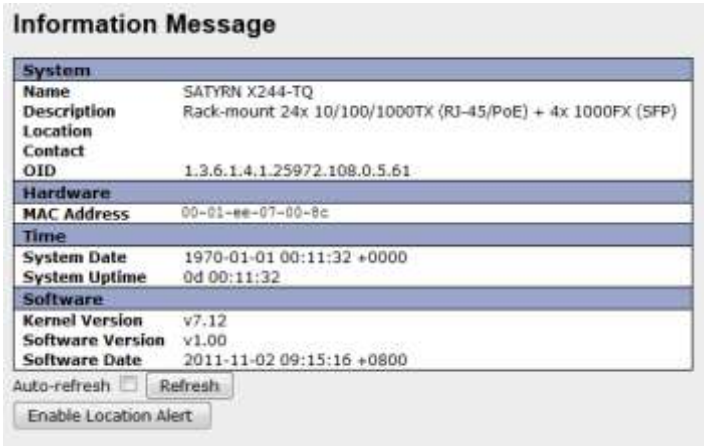
5.4 Command Line Interface

The X-Series switches common with all our managed switches can be programmed using a Command Line Interface. Details are available in Section 7.

6 Browser and Satyrn View's Switch Function Interface

6.1 System Information

This contains the basic information about the switch, click here from any part of the interface to return here.



6.1.1 Location Alert

This function helps you physically locate a specific switch by flashing the PWR and Fault lights.

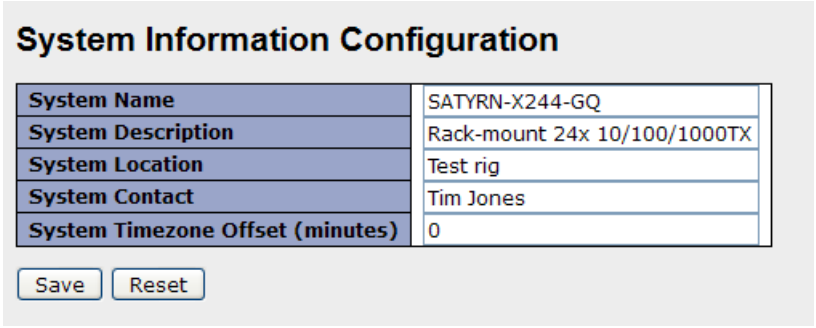
Enable Location Alert switches on the flashing the PWR and Fault lights.

Disable Location Alert switches off the flashing the PWR and Fault lights

6.2 Basic Setting

This is the standard switch setting interface.

6.2.1 Basic Settings

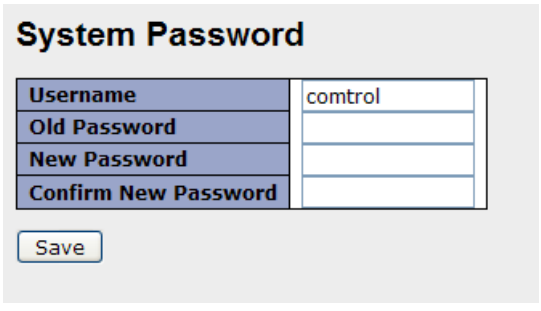


The following table describes the options available.

Option	Description
System Name	Assign the switch name here. Maximum length is 255 characters.
System Description	Displays the switch description.
System Location	Assign the switch's physical location here. The maximum length is 255 characters.
System Contact	Enter the name of a contact person or organization.
Timezone offset	This is the time zone offset relative to UTC/GMT in minutes east of GMT. The valid range is from -720 to +720 minutes.

6.2.2 Admin Password

You can change the Browser management login in user name and pass word here.

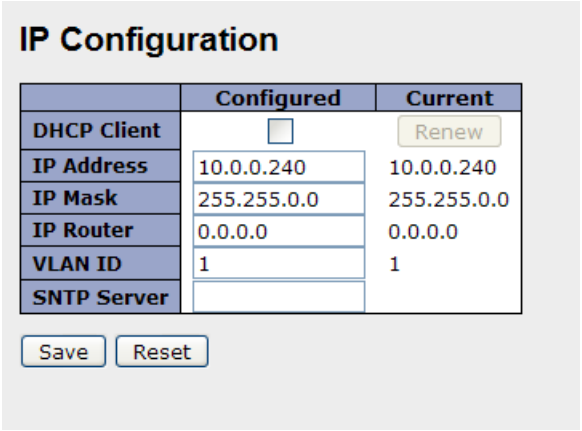


The following table describes the options available.

Option	Description
User name	Enter the new username. (The default is "**comtrol**")
Old Password	Enter the current system password. If this is incorrect, the new password will not be set
New Password	Enter the new password. (The default is "**satyrn**") The maximum length is 31 characters.
Confirm password	Re-type the new password.
Save	Click "**Save**" to save changed configuration settings

6.2.3 IP Setting

You can configure the IP Settings and DHCP client function here.



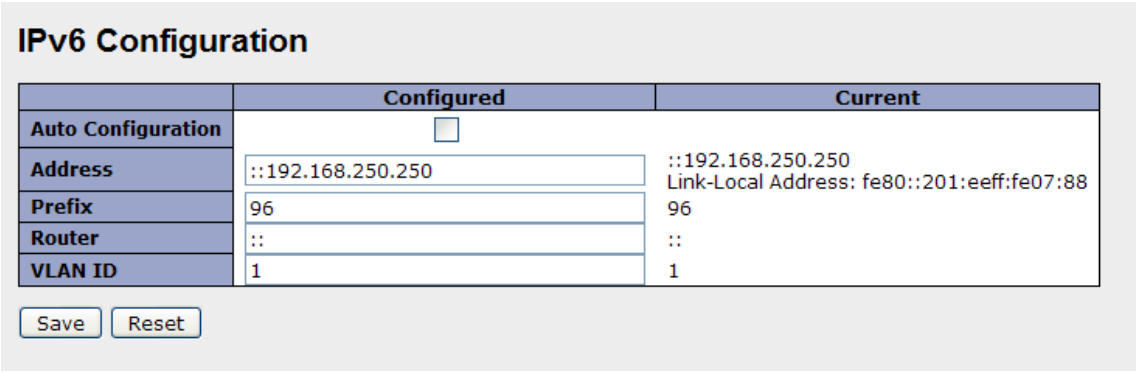
The following table describes the options available.

Option	Description
DHCP Client	Enable or disable the DHCP client function. When the DHCP client function is enabled, the switch will be assigned the IP address from the network DHCP server and the default IP address will be replaced by the IP address which the DHCP server has assigned. If DHCP fails and the configured IP address is zero, DHCP will try again. If DHCP fails and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as the hostname to provide DNS lookup.
IP Address	Assign the IP address used by the network. If the DHCP client function is enabled, you do not need to assign an IP address. The network DHCP server will assign the switch's IP address and it will be displayed in this column. The default IP address is: 192.168.10.1
IP Mask	Assign the subnet mask of the IP address. If DHCP client

	function is enabled, you do not need to assign the subnet mask
IP Router	The network gateway for the switch. The default gateway is 192.168.10.254
VLAN ID	The managed VLAN ID. The allowed range is 1 through 4095.
SNTP Server	This is the IP address of the SNTP server
Save	Click to save changes.
Reset	Click to undo any local changes and restore the previously saved settings.
Renew	Click to renew DHCP. This button is only available if DHCP is enabled.

6.2.4 IPv6 Setting

You can configure the IPv6 Settings here.

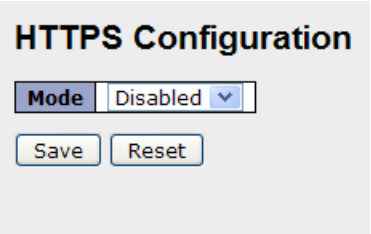


The following table describes the options available.

Option	Description
Auto configuration	Enable or disable the IPv6 auto-configuration. If it fails, the configured IPv6 address is set to zero. The switch may delay responding to a router request for a few seconds, the total time needed to complete auto-configuration can be significantly longer.
IP Address	Provide the IP address used by the network.
Prefix	Provide the IPv6 prefix for this switch
Router	Provide the IPv6 network gateway address for this switch.
VLAN ID	Provide the managed VLAN ID. The allowed range is 1 through 4095.
Save	Click to save changes.
Reset	Click to undo any local changes and restore the previously saved settings.

6.2.5 HTTPS

You can configure the HTTPS settings here.

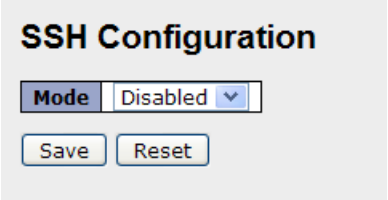


The following table describes the options available.

Option	Description
Mode	Enable or disable the HTTPS mode
Save	Click to save changes.
Reset	Click to undo any local changes and restore the previously saved settings.

6.2.6 SSH

You can configure the SSH settings here.



The following table describes the options available.

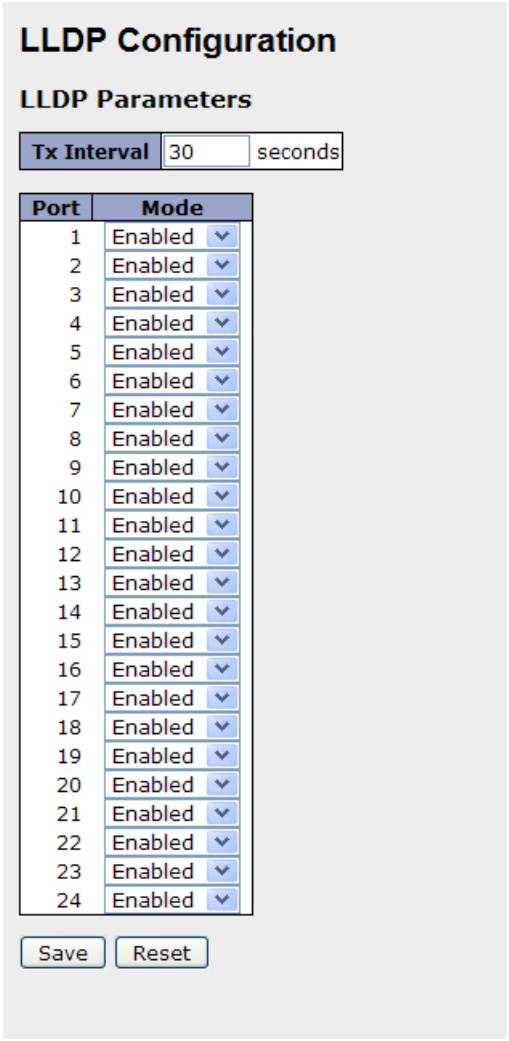
Option	Description
Mode	Enable or disable the SSH mode
Save	Click to save changes.
Reset	Click to undo any local changes and restore the previously saved settings.

6.2.7 LLDP

The LLDP (Link Layer Discovery Protocol) function allows the switch to advertise its information to other nodes on the network and store the information it receives.

6.2.7.1 LLDP Configuration

This page allows you to check and configure the current LLDP port settings.

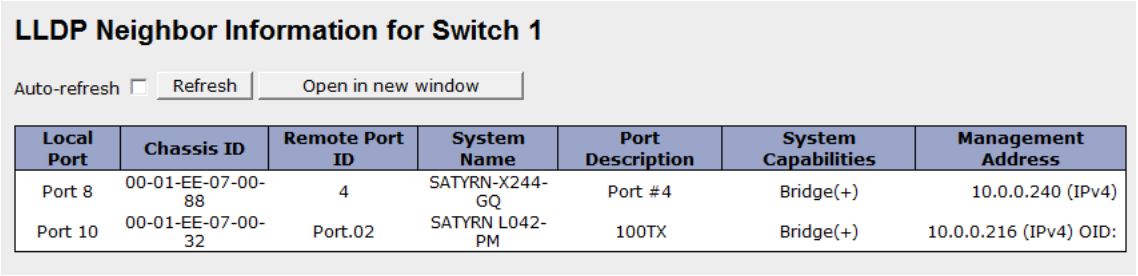


The following table describes the options available.

options	Description
Tx Interval	The interval between each LLDP frame is determined by the Tx Interval value. Valid values are between 5 and 32768 seconds.
Port	The switch port number of the logical LLDP port.
Mode	Enable or disable LLDP

6.2.7.2 LLDP Neighbour Information

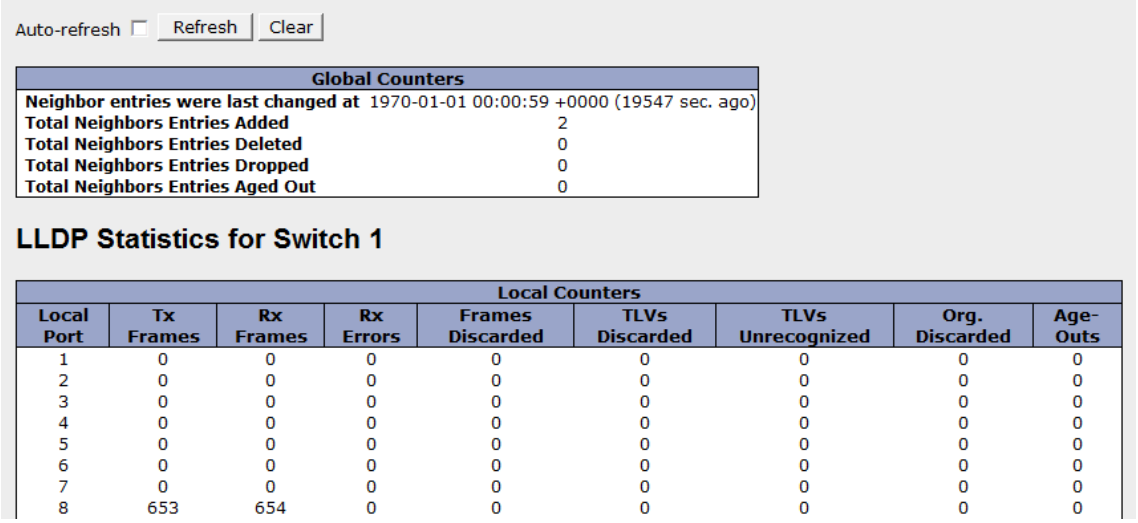
This section provides a status overview for all LLDP neighbours. The displayed table contains a row for each port on which an LLDP neighbour is detected. The columns hold the following information:



Option	Description
Local Port	The LLDP receiving port
Chassis ID	The identification of the neighbour's LLDP frames.
Remote Port ID	The neighbouring port.
System Name	The name of the neighbour unit.
Port Description	The port description of the neighbour unit.
System Capabilities	The neighbour unit's capabilities. The possible capabilities are: 1. Other 2. Repeater 3. Bridge 4. WLAN Access Point 5. Router 6. Telephone 7. DOCSIS cable device 8. Station only 9. Reserved (+) capability enabled (-) capability disabled
Management Address	Neighbouring unit's IP address
Refresh	Click to refresh the page immediately.
Auto refresh	Check this box to enable the automatic refresh of the page at regular intervals.

6.2.7.3 LLDP Statistics

This section provides an overview of all LLDP traffic. Two sorts of counters are shown. Global counters are counters that refer to the whole stack, switch, while local counters refer to counters for the currently selected switch.



Auto-refresh ☐ Refresh Clear

Global Counters	
Neighbor entries were last changed at	1970-01-01 00:00:59 +0000 (19547 sec. ago)
Total Neighbors Entries Added	2
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

LLDP Statistics for Switch 1

Local Counters								
Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	653	654	0	0	0	0	0	0

Global Counters

Options	Description
Neighbour entries were last changed at	The time for when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.
Total Neighbours Entries Added	The number of new entries added since the last switch reboot.
Total Neighbours Entries Deleted	The number of new entries deleted since the last switch reboot.
Total Neighbours Entries Dropped	The number of LLDP frames dropped due to the entry table being full.
Total Neighbours Entries Aged Out	The number of entries deleted due to the expiration of Time-To-Live.

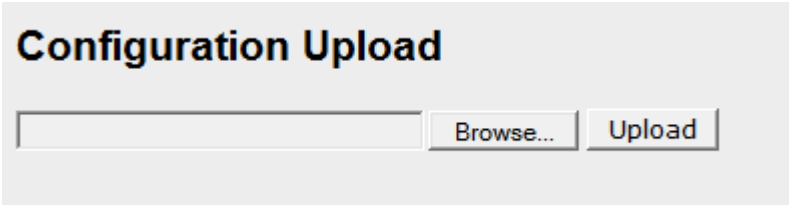
Local Counters

Label	Description
Local Port	The port on which LLDP frames are received or transmitted.
Tx Frames	The number of LLDP frames transmitted on the port.
Rx Frames	The number of LLDP frames received on the port.
Rx Errors	The number of received LLDP frames containing some kind of error.

Frames Discarded	If an LLDP frame is received on a port, and the switch's internal table is full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbours". LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when the related port links down, an LLDP shutdown frame is received, or when the entry ages out.
TLVs Discarded	Each LLDP frame contains multiple pieces of information, known as TLVs (Type Length Value). If a TLV is malformed, it is counted and discarded.
TLVs Unrecognized	The number of correctly formed TLVs containing an unknown type value.
Org. Discarded	The number of organization TLVs received.
Age-Outs	Each LLDP frame contains information about how long the LLDP information is valid (age-out time). If no new LLDP frame is received within the age-out time, the LLDP information is removed and the Age-Out counter is incremented.
Refresh	Click to refresh the page immediately.
Clear	Clears the local counters. All counters (including global counters) are cleared upon reboot.
Auto refresh	Check this box to enable the automatic refresh of the page at regular intervals.

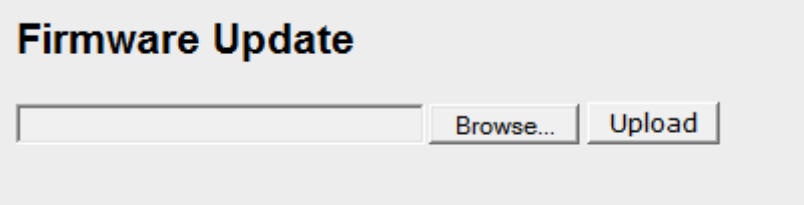
6.2.8 Backup/Restore Configuration

You can view, save, or load the switch configuration. The configuration file is in XML format and contains a hierarchy of tags:



6.2.9 Upgrade Firmware

Upgrade Firmware allows you to update the switch's firmware. Before updating, be sure to have your TFTP server ready and the firmware image available on the TFTP server.

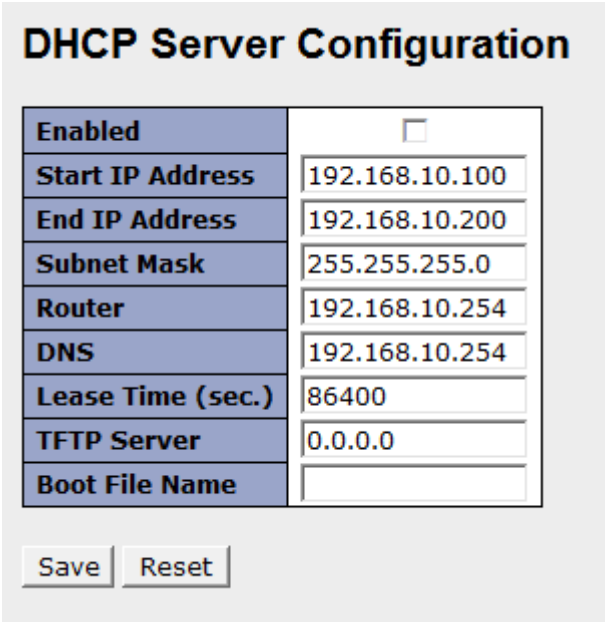


6.3 DHCP Server

The system is provided with DHCP server function

6.3.1 Setting

The X Series switches can operate as a DHCP server. This section allows you to select this mode and select various parameters.

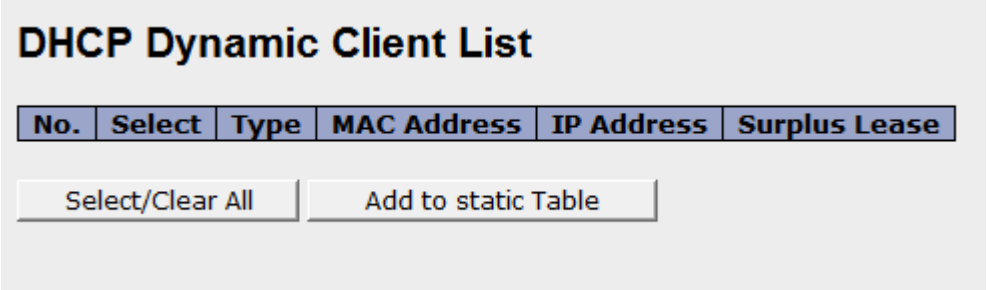


Option	Description
Enabled	Click to Enable or Disable the DHCP Server function. When enabled, the switch will act as the DHCP server on the local network
Start IP Address	The lower limit of the dynamic IP address range. The lower IP address is the beginning of the dynamic IP address range. For example, if the dynamic IP address range is from 192.168.1.100 to 192.168.1.200, then 192.168.1.100 will be the start IP address.
End IP Address	The upper limit of the dynamic IP address range. The highest IP address is the end of the dynamic IP address range. For example, if the dynamic IP address range is from 192.168.1.100

	to 192.168.1.200, then 192.168.1.200 will be the End IP address
Subnet Mask	The subnet mask for the dynamic IP address range.
Router	The IP address of the router
DNS	The IP address of the Domain Name Server.
Lease Time (Sec)	The time at which the system will reset the assigned dynamic IP to ensure the IP address is in use.
Save	Click "**Save**" to save the changed configuration.

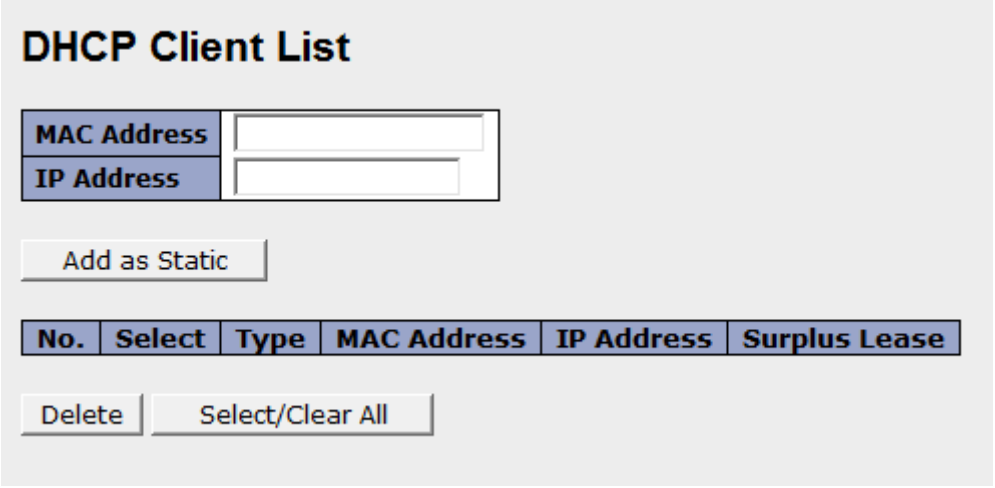
6.3.2 DHCP Dynamic Client List

When the DHCP server function is activated, the system will collect the DHCP client information and display it here.



6.3.3 DHCP Static Client

You can assign a specific IP address in the assigned dynamic IP range to a specific port. When a device is connecting to the port and requests a dynamic IP assignment, the system will assign the specific IP address allocated to that port.

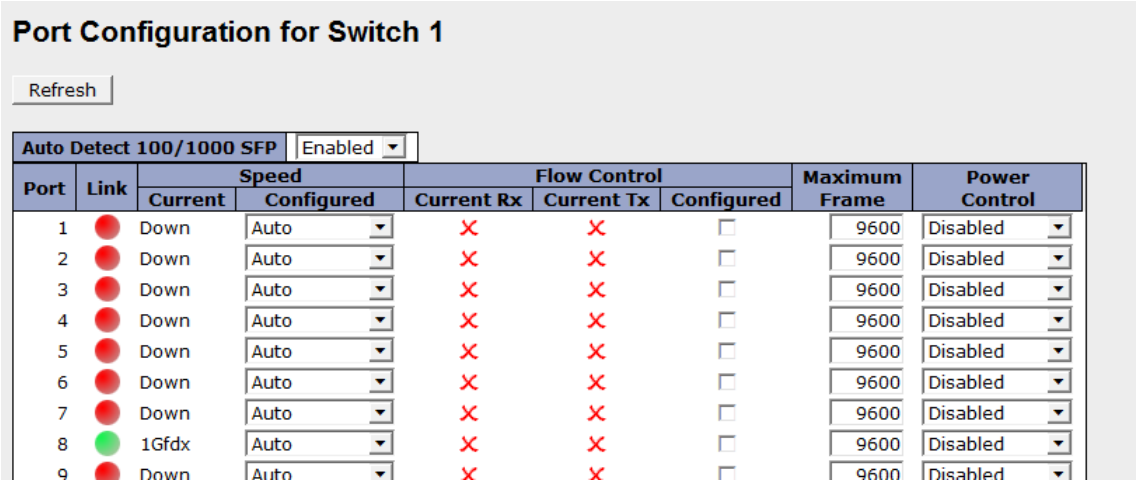


6.4 Port Setting

This section enables you to assign specific parameters to each individual port.

6.4.1 Port Configuration

The Port Configuration function allows you to set the state, speed/duplex, flow control, and security of the individual ports.



Option	Description
Auto Detect 100/1000 SFP	When this function is enabled, the fibre port can auto detect the SFP Module.
Port	The logical port number.
Link	The current link state. Green - link is up Red - link is down.
Current Link Speed	The current link speed of the port.
Configured Link Speed	Select any available link speed for the given switch port. Auto Speed selects the highest speed compatible with the link partner. Disabled means that the switch port will not operate.
Flow Control	When Auto Speed is selected, this indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that speed will be used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column shows whether pause frames on the port are transmitted or not. The Rx and Tx settings are determined by the result of the last Auto-Negotiation. Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.
Maximum Frame	The maximum frame size allowed for the switch port, including FCS. The allowed range is 1518 bytes to 9600 bytes.
Power Control	The Usage column shows the current percentage of the power

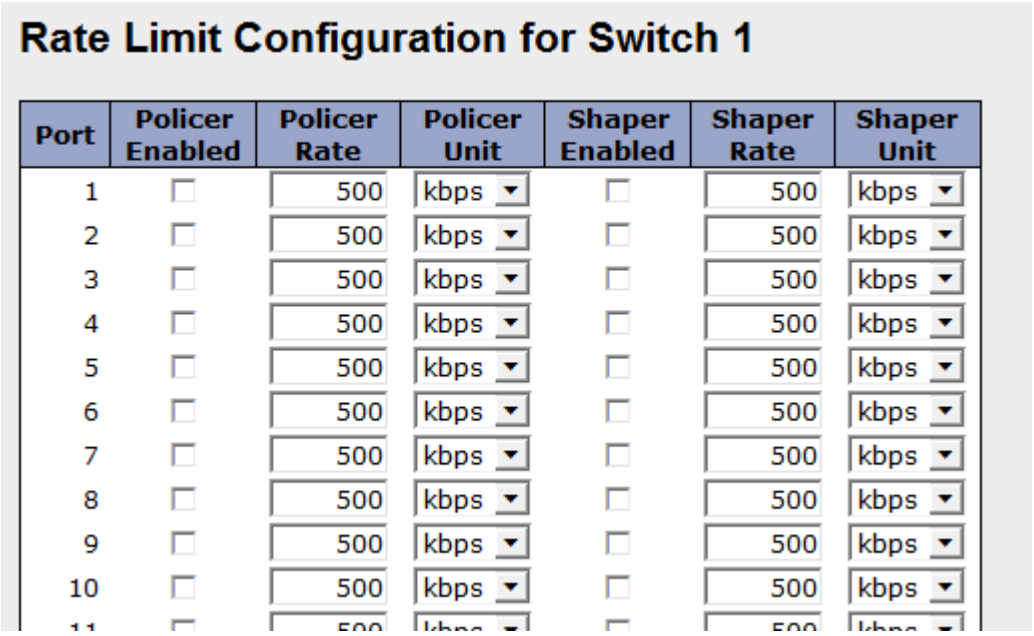
	consumption per port. The Configured column allows for changing the power savings mode parameters per port. Disabled: All power savings mechanisms are disabled. ActiPHY: Link down power savings are enabled. PerfectReach: Link up power savings aare enabled. Enabled: Both link up and link down power savings are enabled.
Save	Click to save changes.
Reset	Click to undo any local changes and restore the previously saved settings.

6.4.2 Rate Limit

This section is used to control the received and transmitted rate on each port. This can be used to prevent excessive data rates on particular ports.

Policer – Controlling the rate of Received frames

Shaper – Controlling the rate of Transmitted frames



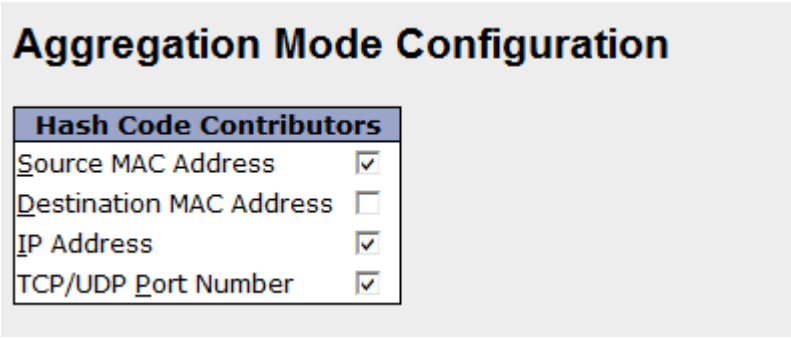
Option	Description
Port	The logical port number.
Policer Enabled	Enable or disable the port policer. The default value is "Disabled".
Policer Rate	Configure the rate for the port policer. The default value is "500". This value is restricted to 500-1000000 when the "Policer Unit" selected is "kbps", and it is restricted to 1-1000 when the "Policer Unit" is "Mbps"

Policer Unit	Configure the unit of measure for the port policer rate as kbps or Mbps. The default value is "kbps".
Shaper Enabled	Enable or disable the port shaper. The default value is "Disabled".
Shaper Rate	Configure the rate for the port shaper. The default value is "500". This value is restricted to 500-1000000 when the "Policer Unit" selected is "kbps", and it is restricted to 1-1000 when the "Policer Unit" is "Mbps"
Shaper Unit	Configure the unit of measure for the port shaper rate as kbps or Mbps. The default value is "kbps".
Save	Click to save changes.
Reset	Click to undo any local changes and restore the previously saved settings.

6.4.3 Port Trunk

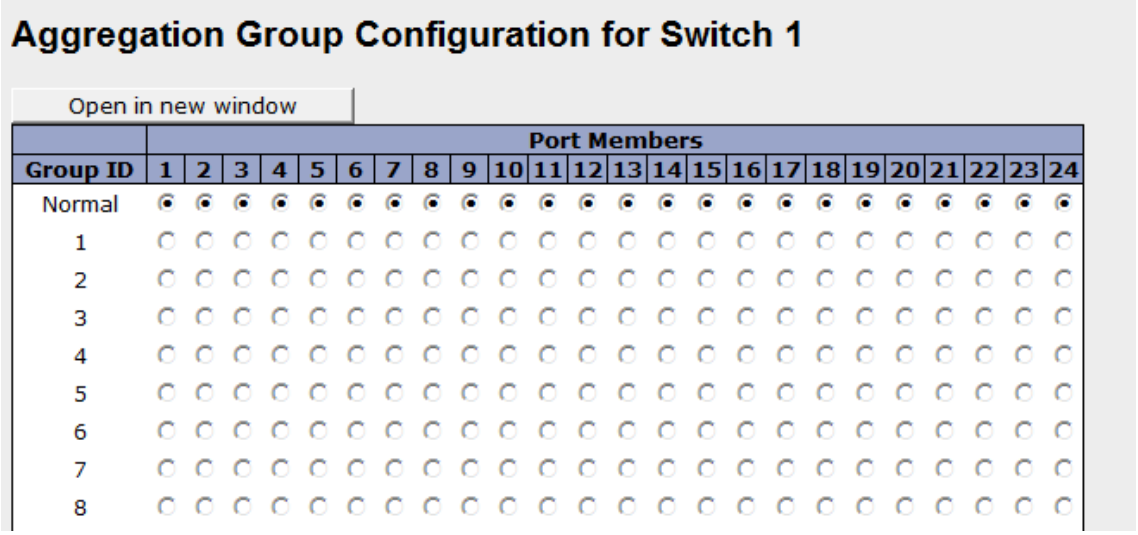
A port trunk enables you to aggregate multiple ports in parallel to increase the link speed beyond the limits of a single port and to increase the redundancy for higher availability across the aggregated ports.

This page is used to configure the aggregation hash mode and the aggregation group.



Option	Description
Source MAC Address	The Source MAC address is used to calculate the destination port for the frame. Check this box to enable the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled.
Destination MAC Address	The Destination MAC Address is used to calculate the destination port for the frame. Check this box to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled.

IP Address	The IP address is used to calculate the destination port for the frame. Check this box to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled.
TCP/UDP Port Number	The TCP/UDP port number is used to calculate the destination port for the frame. Check this box to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled.

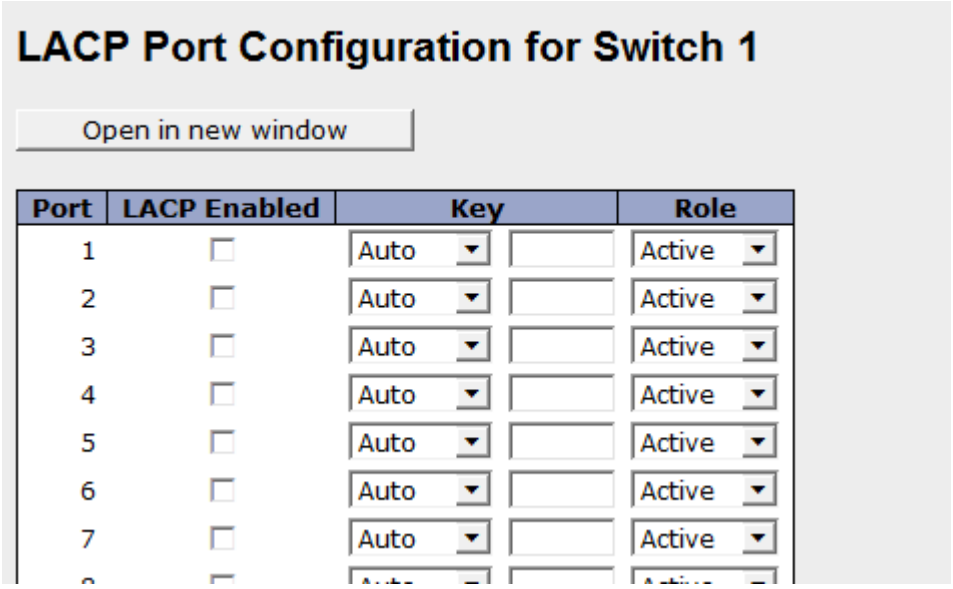


Option	Description
Group ID	Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.
Port Members	Each switch port is listed for each group ID. Check a radio button to include a port in an aggregation, or uncheck the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and all ports must be set to the same speed in each group.

6.4.3.1 LACP Port Configuration

The Link Aggregation Control Protocol, allows bundling several physical ports together to form a single logical port.

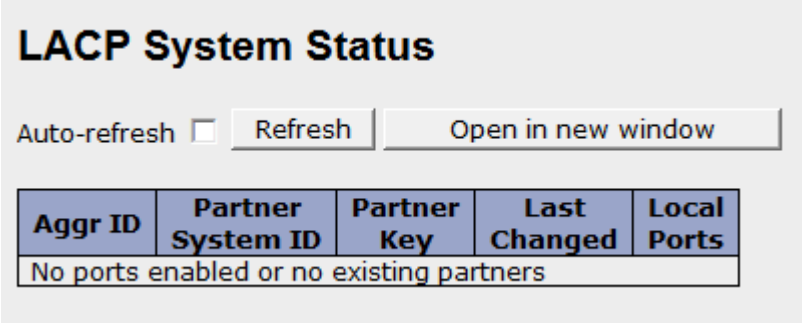
This page allows the user to view and configure the LACP port settings.



Option	Description
LACP Enabled	To enable LACP for the port check the box.
Key	The Key value allocated to the port in the range 1-65535. The Auto setting will set the key as appropriate to the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. A user-defined value can also be entered in the adjacent box. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.
Role	The Role shows the LACP activity status. If set to Active the port will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner.
Save	Click to save changes.
Reset	Click to undo any local changes and restore the previously saved settings.

6.4.3.2 LACP System Status

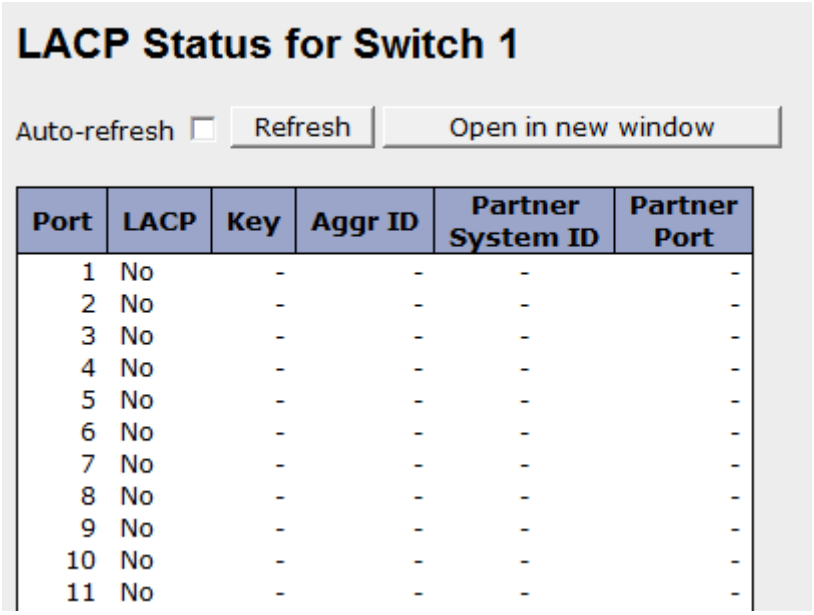
This page provides a status overview for all the LACP instances.



Option	Description
Aggr ID	The Aggregation ID associated with this aggregation instance. For LLAG the ID is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'
Partner System ID	The system ID (MAC address) of the aggregation partner.
Partner Key	The Key that the partner has assigned to this aggregation ID.
Last Changed	The time since this aggregation changed.
Local Ports	Shows which ports are a part of this aggregation for this switch/stack. The format is: "Switch ID:Port".
Refresh	Click to refresh the page immediately.
Auto Refresh	Check this box to enable an automatic refresh of the page at regular intervals.

6.4.3.3 LACP Status

This page provides a status overview for LACP status for all the ports.

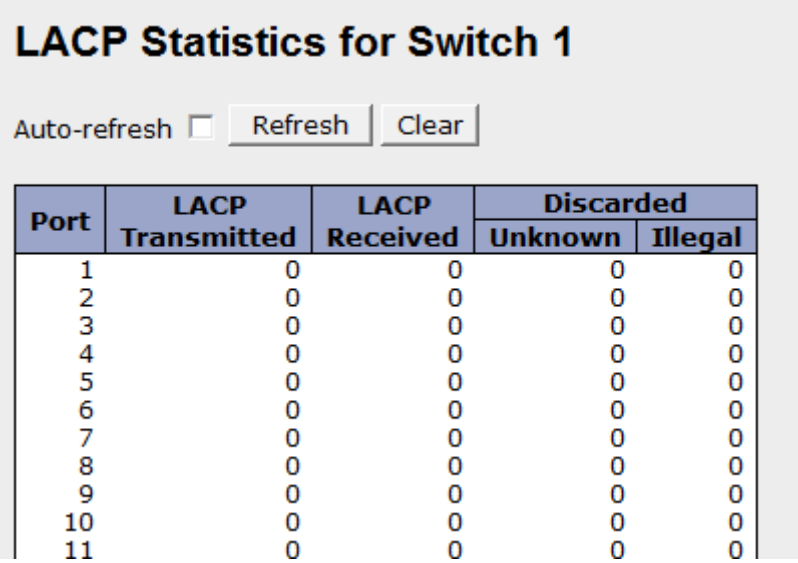

LACP Status for Switch 1
Auto-refresh
Refresh
Open in new window
Port LACP Key Aggr ID Partner System ID Partner Port
1 No - - - -
2 No - - - -
3 No - - - -
4 No - - - -
5 No - - - -
6 No - - - -
7 No - - - -
8 No - - - -
9 No - - - -
10 No - - - -
11 No - - - -

Option	Description
Port	The switch port number.
LACP	Yes LACP is enabled and the port link is up No LACP is not enabled or that the port link is down Backup Port could not join the aggregation group but will join if another port leaves. In the meantime, its LACP status is disabled.
Key	The key assigned to this port. Only ports with the same key can aggregate together.

Aggr ID	The Aggregation ID assigned to this aggregation group.
Partner System ID	The partners System ID (MAC address).
Partner Port	The partners port number connected to this port.
Refresh	Click to refresh the page immediately.
Auto Refresh	Check this box to enable an automatic refresh of the page at regular intervals.

6.4.3.4 LACP Statistics

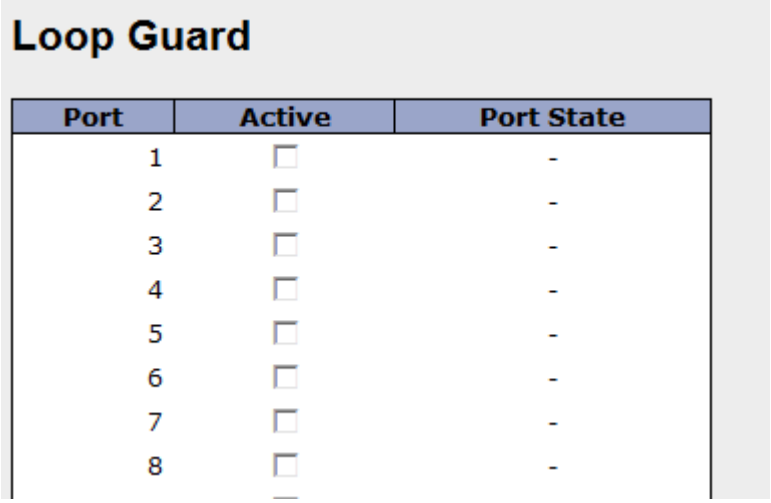
This page provides an overview for LACP statistics for all the ports.



Option	Description
Port	The switch port number
LACP Transmitted	Shows how many LACP frames have been sent from each port
LACP Received	Shows how many LACP frames have been received by each port.
Discarded	Shows how many unknown or illegal LACP frames have been discarded at each port.
Refresh	Click to refresh the page immediately.
Auto Refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Clear	Clears the counters for all ports

6.4.4 Loop Guard

Loop Guard is a looping detection/avoidance strategy, it helps network administrators avoid a looping issue.

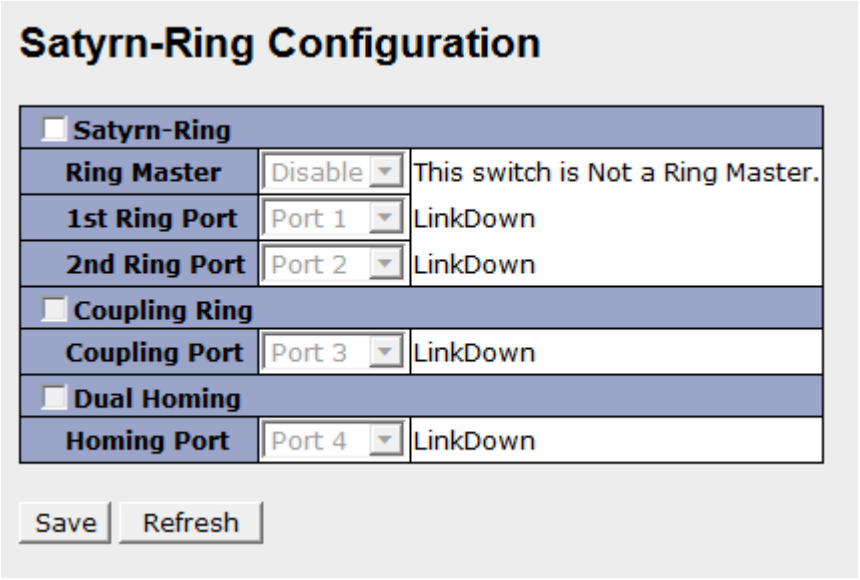


Option	Description
Active	Enable Loop Guard function
Port State	Guarding This port is protected against looping. Locked This port has been locked to avoid looping.

6.5 Redundancy

6.5.1 Satyrn-Ring

Satyrn-Ring features one of the most powerful redundant ring technologies. The recovery time of Satyrn-Ring is less than 10 mS over 250 units of connections. This redundancy can reduce unexpected malfunctions caused by changes to the network topology. Satyrn-Ring technology supports three ring topologies for network redundancy: Satyrn-Ring, Coupling Ring and Dual Homing.



The following table describes the options available.

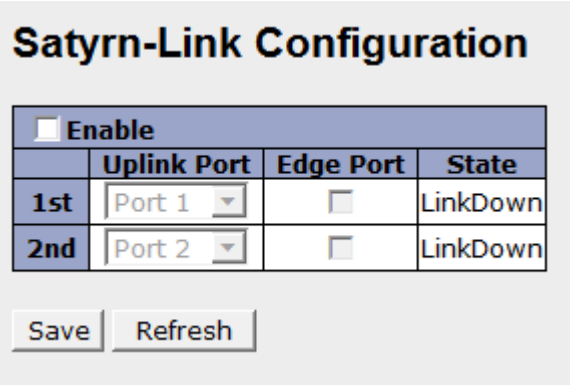
Option	Description
Satyrn-Ring	Check box to enable Satyrn-Ring.
Ring Master	There should be only one Ring Master in a ring. However if there are two or more switches for which Ring Master is enabled, the switch with the lowest MAC address will serve as the Ring Master and others will serve as Backup Masters.
1st Ring Port	The Ring Master's primary port.
2nd Ring Port	The Ring-Master's secondary port.
Coupling Ring	Check box to enable Coupling Ring. Coupling Ring can be used to divide a big ring into two smaller rings to prevent network topology changes from affecting all the switches.. It is useful for connecting two Satyrn-Rings.
Coupling Port	Link to Coupling Port of the switch in another ring. A Coupling Ring needs four switches to build active and backup links. Set a port as coupling port. The coupled four ports of four switches will be run in active/backup mode.
Control Port	Link to Control Port of the switch of the same ring. Control Port used to transmit control signals.
Dual Homing	Check box to enable Dual Homing. By selecting Dual Homing mode, Satyrn-Ring will be connected to normal switches through two RSTP links (ex: backbone Switch). The two links work in active/backup mode and connect each Satyrn-Ring to the normal switches in RSTP mode.
Apply	Click "**Apply**" to save the changed configuration settings.

Note: Do not set one switch as both a Ring Master and a Coupling Ring at the same time as this will place a heavy load on the network.

6.5.2 Satyrn Link

Satyrn Link allows you to add on network redundancy topology for any backbone network. This enables multiple redundant network rings to combine together and function as a larger more robust network.

Satyrn Link only requires the edge port of the edge switch to be identified with other switches in the ring set with Satyrn Link enabled.



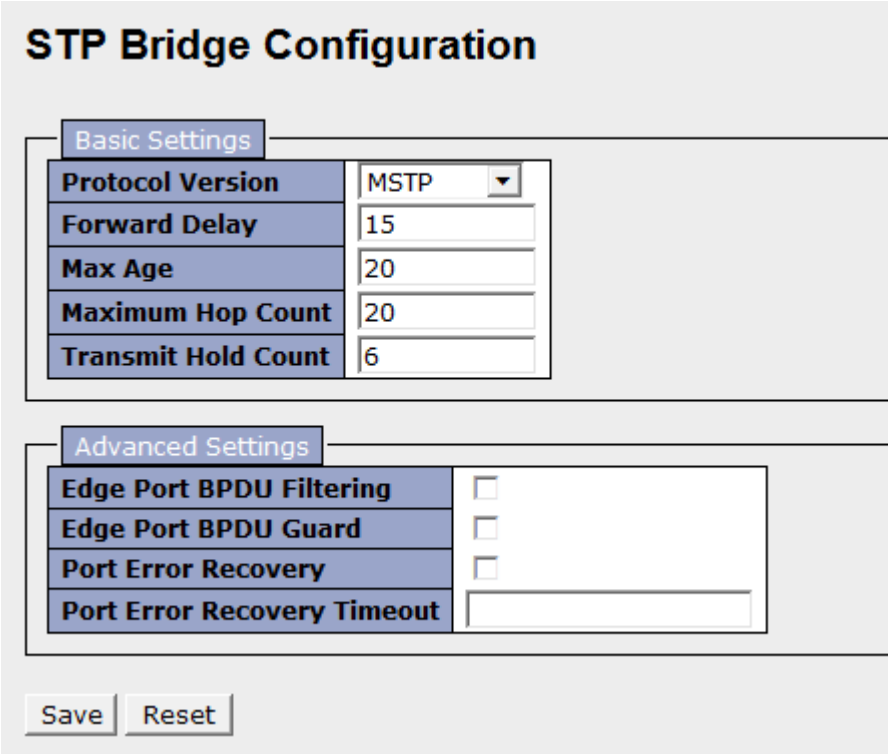
The following table describes the options available.

Option	Description
Enable	Enable the Satyrn-Link function.
Uplink Port	Select the appropriate port for 1st or 2nd uplink port
Edge Port	Select the port connected to the main riing
Apply	Apply the selected settings

6.5.3 MSTP

6.5.3.1 Bridge settings

This page allows you to configure the RSTP system settings. These settings are used by all of the RSTP Bridge instances in the Switch Stack.



The following table describes the basic settings available.

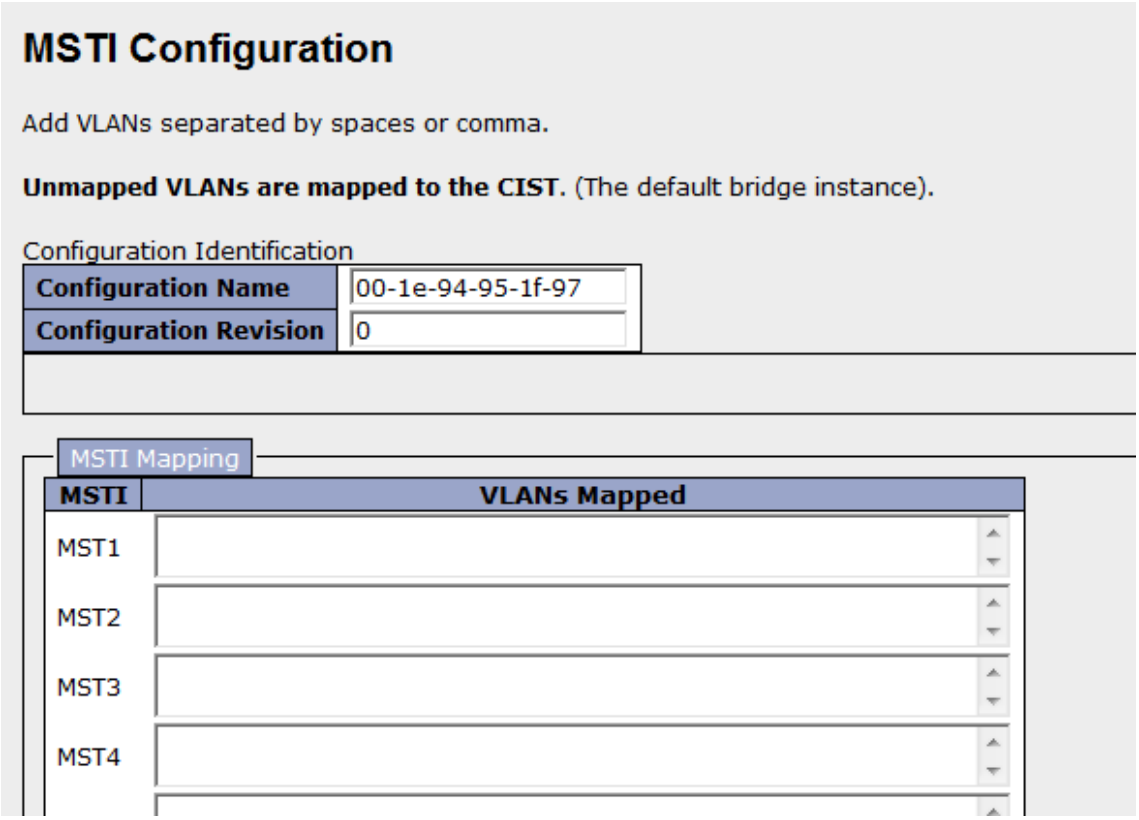
Option	Description
Protocol Version	The STP protocol version setting. The valid values are STP, RSTP and MSTP.
Forward Delay	The delay used by STP Bridges to change Root and Designated Ports to Forwarding (used in STP compatible mode). The valid values are from 4 to 30 seconds.
Max Age	The maximum age of the information transmitted by the Bridge when it is the Root Bridge. The valid values are from 6 to 40 seconds and the MaxAge must be <= (FwdDelay-1)*2.
Maximum Hop Count	This defines the initial value of the remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information. The valid values are from 4 to 30 seconds and the MaxAge must be <= (FwdDelay-1)*2.
Transmit Hold Count	The number of BPDUs per second a bridge port is permitted to send. When this value is exceeded, the transmission of the next BPDU will be delayed. The valid values are from 1 to 10 BPDU's per second.
Save	Click to save changes.
Reset	Click to undo any local changes and restore the previously saved settings.

The following table describes the advanced settings available.

Option	Description
Edge port BDPU Filtering	Controls whether a port is *explicitly* configured as an Edge and will transmit and receive BPDUs.
Edge port BDPU Guard	Controls whether a port *explicitly* configured as an Edge and will disable itself upon reception of a BPDU. The port will enter the *error-disabled* state, and will be removed from the active topology
Port error recovery	Controls whether a port in the *error-disabled* state will automatically be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.
Port error recovery timeout	The timeout before a port in the *error-disabled* state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).
Save	Click to save changes.
Reset	Click to undo any local changes and restore the previously saved settings.

6.5.3.2 MSTI mapping

This page allows the user to inspect and configure the current STP MSTI bridge instance priority settings.

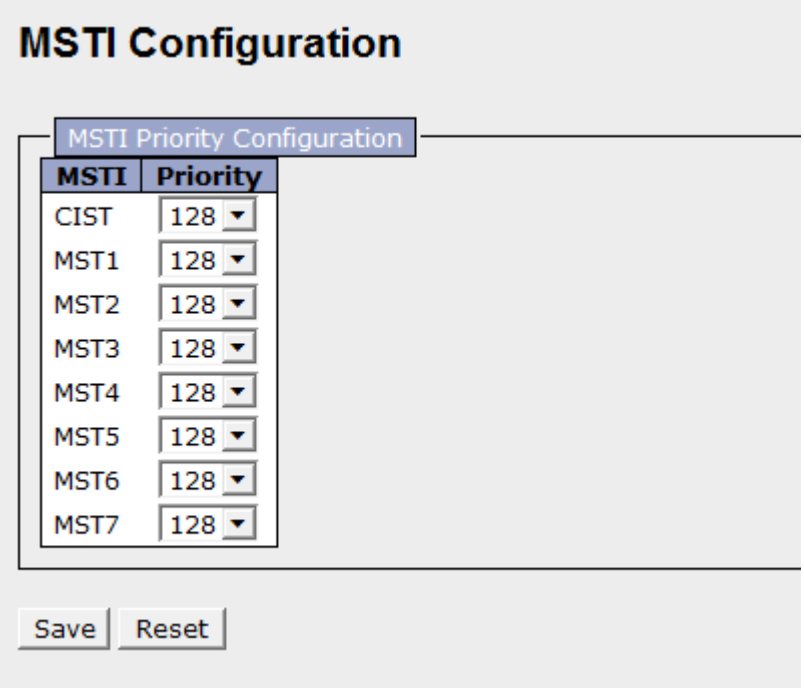


The following table describes the options available.

Option	Description
Configuration Name	The name identifying the VLAN to MSTI mapping. Bridges must share the same name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTIs. (Intra-region). The longest permissible name is 32 characters.
Configuration Revision	The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.
MSTI	The bridge instance. The CIST is not available for explicit mapping as it will receive the VLANs which are not explicitly mapped.
VLANS Mapped	The list of VLAN's mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. A unused MSTI should be left empty; without any VLANs mapped to it.
Save	Click to save changes.
Reset	Click to undo any local changes and restore the previously saved settings.

6.5.3.3 MSTI priorities

This page allows you e user to inspect and configure the current STP MSTI bridge instance priority settings.

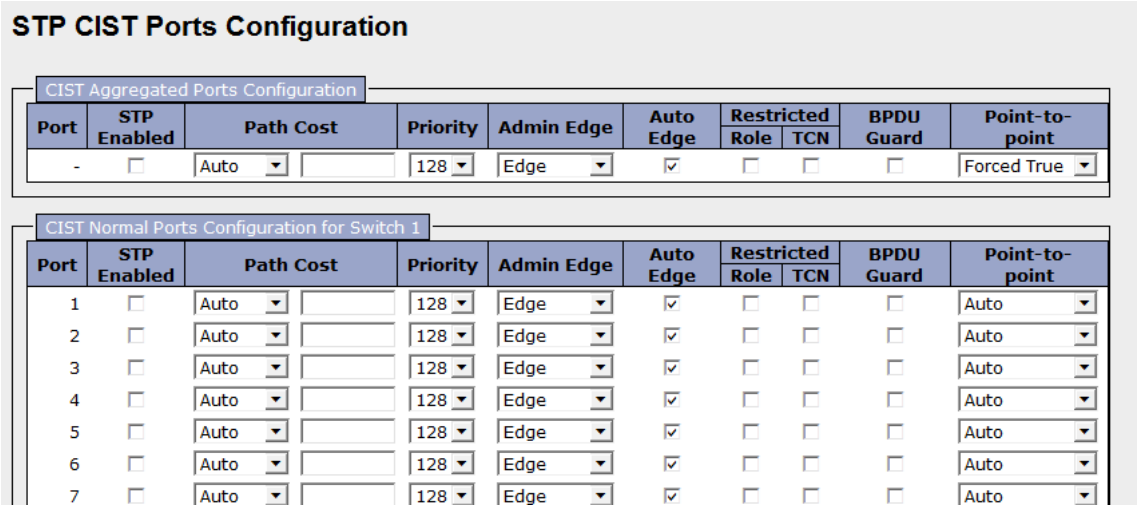


The following table describes the options available.

Option	Description
MSTI	The bridge instance. The CIST is the default instance and is always active.
Priority	The bridge priority control. Lower numerical values have higher priority. The bridge priority plus the MSTI instance number, along with the 6-byte MAC address of the switch, forms a Bridge Identifier.
Save	Click to save changes.
Reset	Click to undo any local changes and restore the previously saved settings.

6.5.3.4 CIST ports

This page allows the user to inspect and configure the current STP CIST port settings. This page contains settings for both physical and aggregated ports. The aggregation settings are stacked globally.



The following table describes the options available.

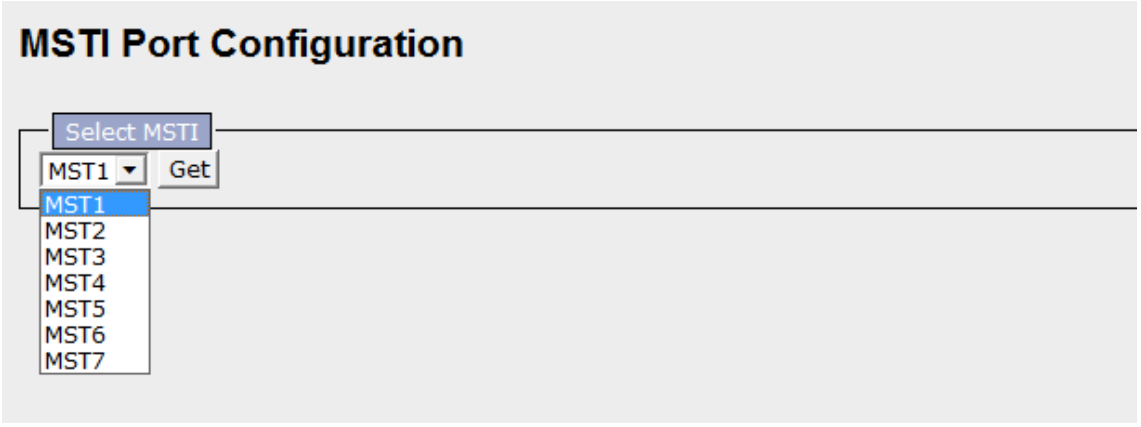
Option	Description
Port	The switch port number of the logical STP port.
STP Enabled	Enable/disable STP on this switch port.
Path Cost	The path cost incurred by the port. The auto setting will set the path cost by the physical link speed, using the 802.1D recommended values. Alternatively, a user-defined value can be set using the Specific setting. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values range from 1 to 200000000.

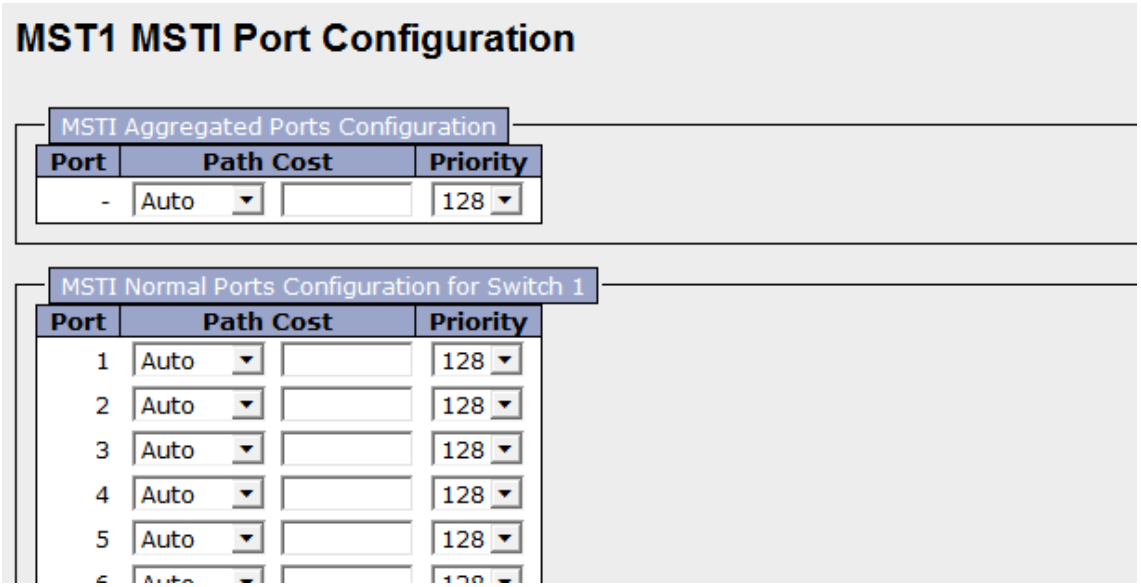
Priority	The port priority setting. This can be used to control priority of ports with identical port costs.
OperEdge(state flag)	Operational flag describing whether the port is connected directly to edge devices. (No Bridges attached). Transitioning to the forwarding state is faster for edge ports (operEdge set to true) than for other ports.
AdminEdge	The initial operEdge state when a port is initialized. The two values are “set” or “cleared”.
AutoEdge	Determines if the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.
Restricted Role	This setting prevents the port from being selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If enabled, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.
Restricted TCN	This causes the port not to propagate received topology change notifications and topology changes to other ports when enabled. It can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect station location information. Restricted TCN is enabled by a network administrator to prevent bridges external to a core region of the network causing address flushing in that region because those bridges are not under the full control of the administrator or because the physical link state for the attached LANs frequently transitions.
Point2Point	Determines whether the port connects to a point-to-point LAN or a shared medium. This can be automatically determined, or specified by the user. Transition to the forwarding state is faster for point-to-point LANs than for shared media.
Save	Click to save changes.
Reset	Click to undo any local changes and revert to previously saved settings.

6.5.3.5 MSTI ports

This page allows the user to inspect and configure the current STP MSTI port settings. A MSTI port is a virtual port, which is established separately for each active CIST (physical) port, for each MSTI instance which is and configured and applicable for that port. The MSTI instance must be selected before the actual MSTI port configuration options are displayed.

This page contains MSTI port settings for physical and aggregated ports. The aggregation settings are stack global.





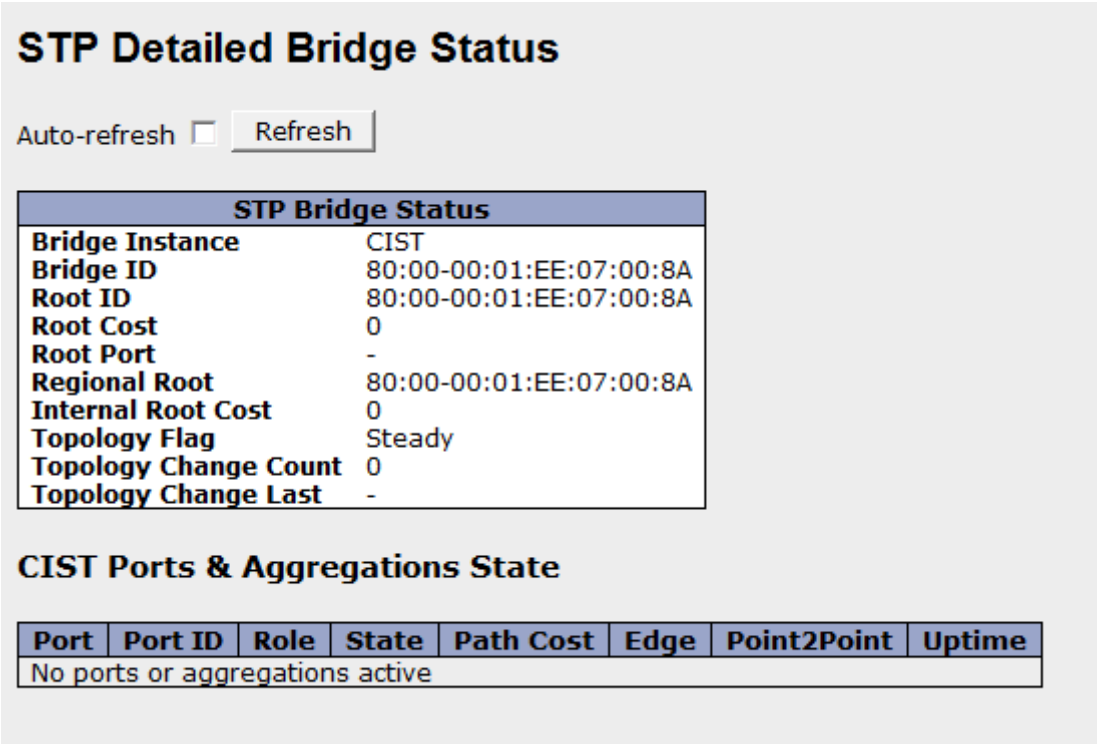
The following table describes the options available.

Option	Description
Port	The switch port number of the corresponding STP, CIST and MSTI port.
Path Cost	The path cost incurred by the port. The auto setting will set the path cost by the physical link speed, using the 802.1D recommended values. Alternatively, a user-defined value can be set using the Specific setting. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values range from 1 to 200000000.
Priority	The port priority setting. This can be used to control priority of ports with identical port costs.
Save	Click to save changes.

Reset	Click to undo any local changes and revert to previously saved settings.

6.5.3.6 Bridge Status

This page provides a status overview for all STP bridge instances. The displayed table contains a row for each STP bridge instance where the column displays the following information:



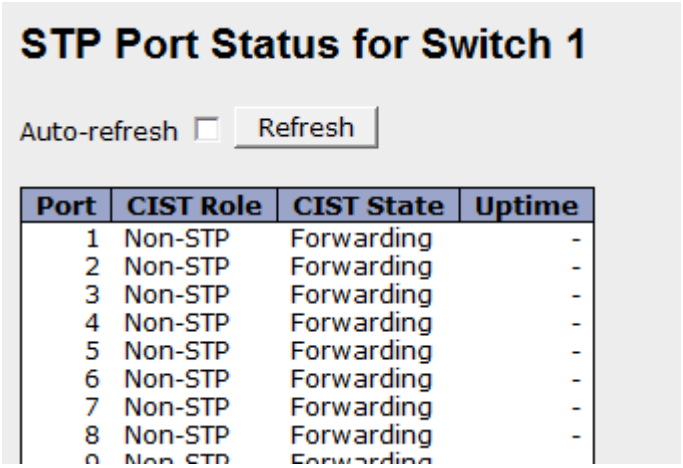
The following table describes the options available.

Option	Description
MSTI	The Bridge Instance. This is also a link to the STP Detailed Bridge Status.
Bridge ID	The Bridge ID of this Bridge instance.
Root ID	The Bridge ID of the currently selected Root Bridge.
Root Port	The switch port currently assigned to be the root port.
Root Cost	Root Path Cost. This is zero for the Root Bridge. For all other Bridges, it is the sum of the Port Path Costs on the smallest cost path to the Root Bridge.
Topology Flag	The current state of the Topology Change Flag for this Bridge instance.
Topology Change Last	The time since the last Topology Change occurred.

Refresh	Click to refresh the page immediately.
Auto Refresh	Check to enable the automatic refresh of the page at regular intervals.

6.5.3.7 STP Port Status

This page displays the STP CIST port status for port physical ports for this switch.

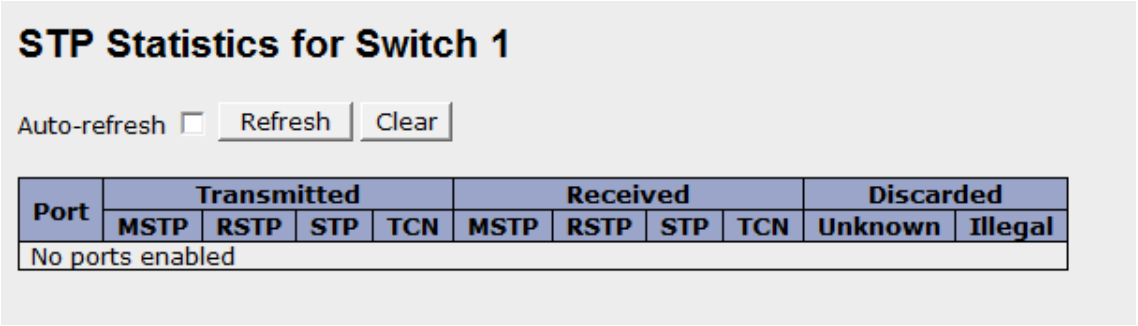


The following table describes the options available.

Option	Description
Port	The switch port number of the logical STP port.
CIST Role	The current STP port role of the CIST port. The port role can be set to one of the following four roles: AlternatePort, BackupPort, RootPort, or DesignatedPort.
State	The current STP port state of the CIST port. The port state can be set to one of the following three settings: Blocking, Learning, or Forwarding.
Uptime	The time since the bridge port was last initialized.
Refresh	Click to refresh the page immediately.
Auto Refresh	Click to enable the automatic refresh of the page at regular intervals.

6.5.3.8 STP Statistics

This page displays the RSTP port statistics counters for bridge ports for this switch.



The following table describes the options available.

Option	Description
Port	The switch port number of the logical RSTP port.
RSTP	The number of RSTP Configuration BPDU's received/transmitted on the port.
STP	The number of legacy STP Configuration BPDUs received/transmitted on the port.
TCN	The number of Topology Change Notification BPDUs received/transmitted on the port.
Discarded Unknown	The number of unknown Spanning Tree BPDU's received/discarded on the port.
Discarded Illegal	The number of illegal Spanning Tree BPDU's received/discarded on the port.
Refresh	Click to refresh the page immediately.
Auto Refresh	Check to enable the automatic refresh of the page at regular intervals.

6.5.4 Fast Recovery

Fast Recovery is a function for port redundancy. The port has the highest recovery priority (the lowest number) will be the active port; others will be blocked (if included).

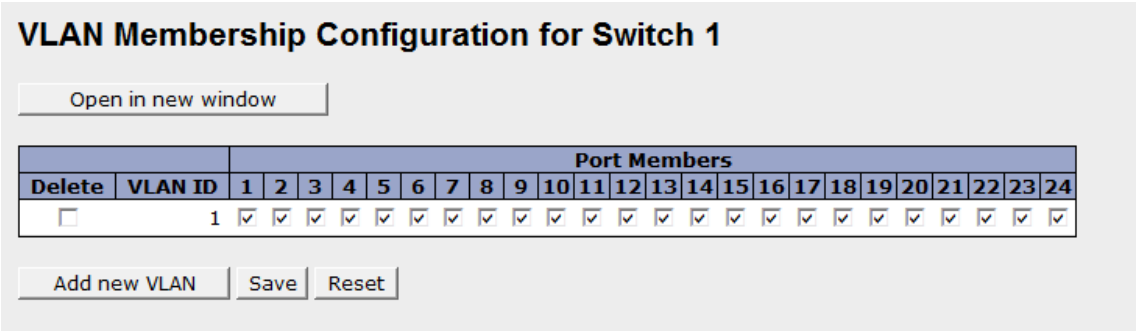
The following table describes the options available.

Option	Description
Enable	Enables Fast Recovery function
Recovery Priority	The port has the highest recovery priority (the lowest number) will be the active port, others will be blocked.

6.6 VLAN

6.6.1 VLAN Membership Configuration

The VLAN membership configuration for the switch is monitored and modified here. Up to 64 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting the port members of each VLAN.

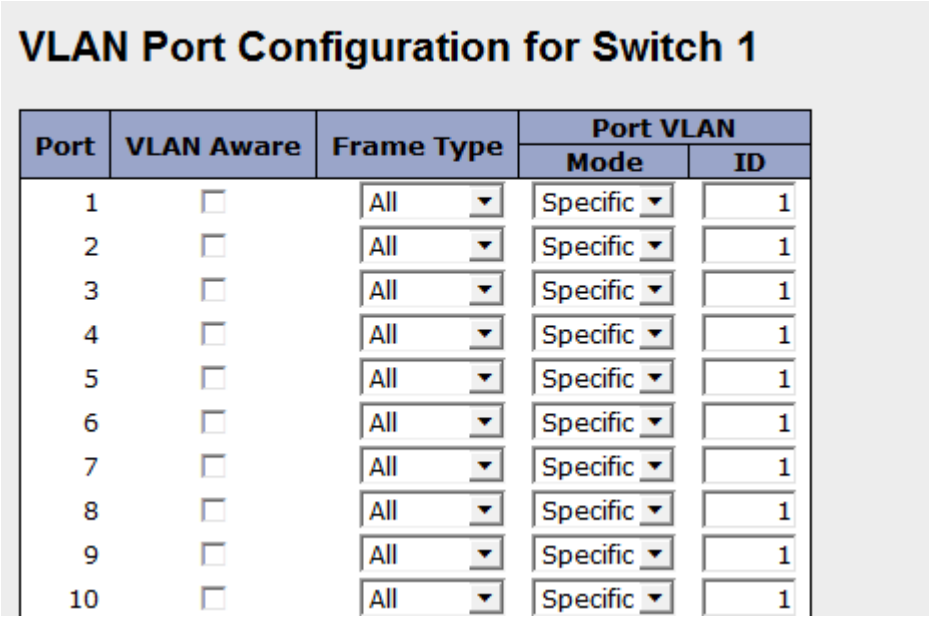

VLAN Membership Configuration for Switch 1
Open in new window
Port Members
Delete
VLAN ID
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
1
Add new VLAN
Save
Reset

The following table describes the options available.

Options	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID for the entry.
MAC Address	The MAC address for the entry.
Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to change the port status.
Adding a New Static Entry	Click 'Add new VLAN' to add a new VLAN ID. An empty row is added to the table, and the VLAN can be configured as required. Valid values for a VLAN ID range from 1 to 4095. The VLAN is enabled on the selected stack switch unit when you click "Save". The VLAN will thereafter be present on the other stack switch units, but without any port members. A VLAN without any port members on a stack unit will be deleted when you click "Save". The 'Delete' button is used to remove unwanted VLANs.

6.6.2 VLAN Port

This page is used for configuring the switch port VLANs.



The following table describes the options available.

Options	Description
Port	This is the logical port number.
VLAN Aware	If VLAN aware is enabled, the tag is removed from tagged frames received on the port and VLAN tagged frames are classified to the VLAN ID in the tag. If VLAN aware is disabled, all frames are classified to the Port VLAN ID and tags are not removed. By default, VLAN aware is disabled.
Frame type	This parameter affects VLAN ingress processing. All – all frames are accepted Tagged - Tagged frames are accepted and untagged frames received at the port are discarded. By default, the field is set to All.
Port VLAN mode	This configures the Port VLAN Mode and affects ingress and egress processing. None - A VLAN tag with the classified VLAN ID is inserted in frames transmitted on the port. This mode is normally used for ports connected to VLAN aware switches. Specific - The Port VLAN ID can be configured (see below). Untagged frames received on the port are classified to the Port VLAN ID. If VLAN awareness is disabled, all frames received on the port are classified to the Port VLAN ID. If the classified VLAN ID of a frame transmitted on the port is different from the Port VLAN ID, a VLAN tag with the classified VLAN ID is inserted in the frame.

Port VLAN ID	Configures the VLAN identifier for the port. The allowed values are 1 through to 4095. The default value is 1. **Note:** The port must be a member of the same VLAN as the Port VLAN ID.

6.6.3 Private VLAN

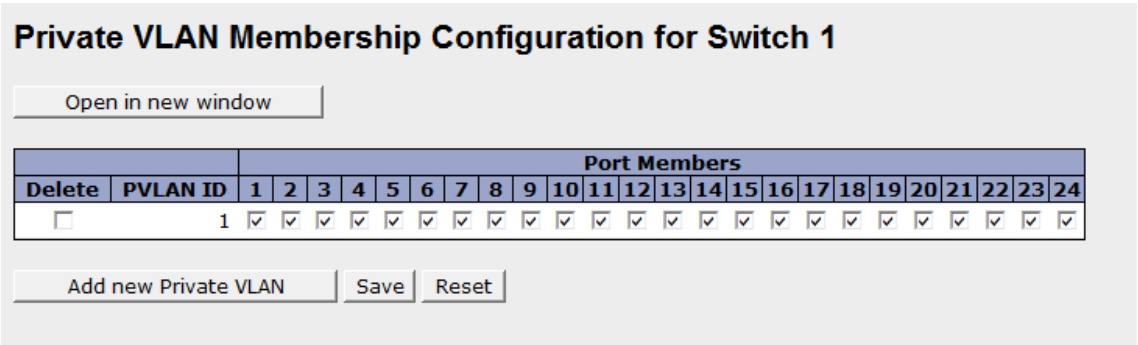
The Private VLAN membership configurations for the switch are monitored and modified here. Private VLANs can be added or deleted. Port members of each Private VLAN can be added or removed. Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical.

A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.

A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

6.6.3.1 Membership

This section is used to configure the membership of a Private VLAN.


Private VLAN Membership Configuration for Switch 1
Open in new window
Port Members
Delete
PVLAN ID
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
1
Add new Private VLAN
Save
Reset

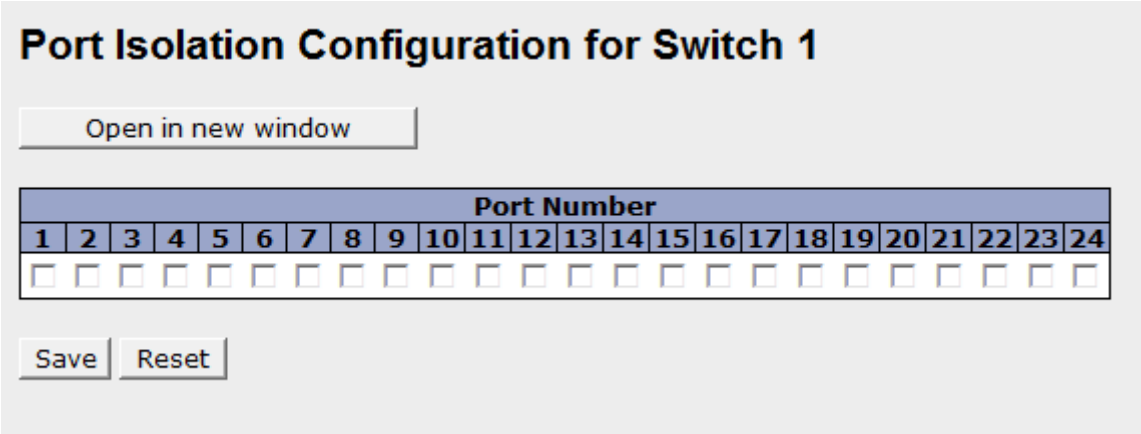
The following table describes the options available.

Option	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Private VLAN ID	The ID of this particular private VLAN.
MAC Address	The MAC address for the entry.
Port Members	A row of check boxes for each port is displayed for each private VLAN ID. Check the box to include a port in a Private VLAN. Uncheck the box to remove or exclude the port from the Private VLAN. By default, all boxes are unchecked and no ports are members.
Adding a New Static Entry	Click 'Add New Private LAN' to add a new private VLAN ID. An empty row is added to the table and the private VLAN can be configured. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range

	are not accepted, and a warning message appears. Click "OK" to discard the incorrect entry, or click "Cancel" to return to the editing and make a correction. The Private VLAN is established when you click "Save". The 'Delete' button will remove unwanted new Private VLANs.

6.6.3.2 Port Isolation

Port isolation is established in this section.


Port Isolation Configuration for Switch 1
Open in new window
Port Number
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Save
Reset

The following table describes the options available.

Label	Description
Port Members	A check box is provided for each port of a private VLAN. When checked, port isolation is enabled for that port. When unchecked, port isolation is disabled for that port. Port isolation is disabled for all ports by default.

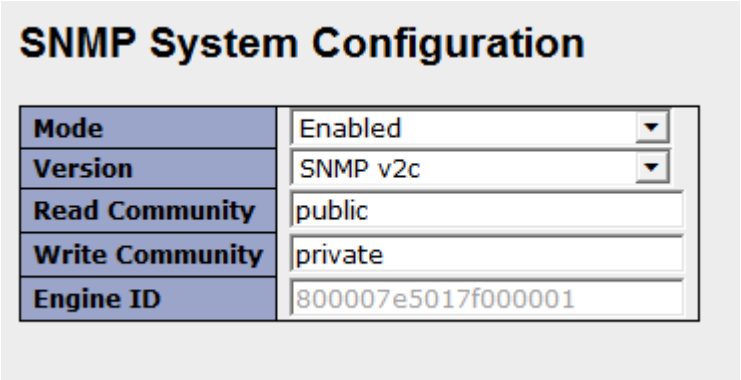
6.7 SNMP

Simple Network Management Protocol (SNMP) is the protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. SNMP enables network administrators to manage network performance, detect and repair network problems, and accommodate network growth. Network management systems are informed of problems by receiving traps, or change notices, from network devices utilizing SNMP.

6.7.1 SNMP-Configuration

6.7.1.1 SNMP-System configuration

Basic SNMP system configuration can be set here.

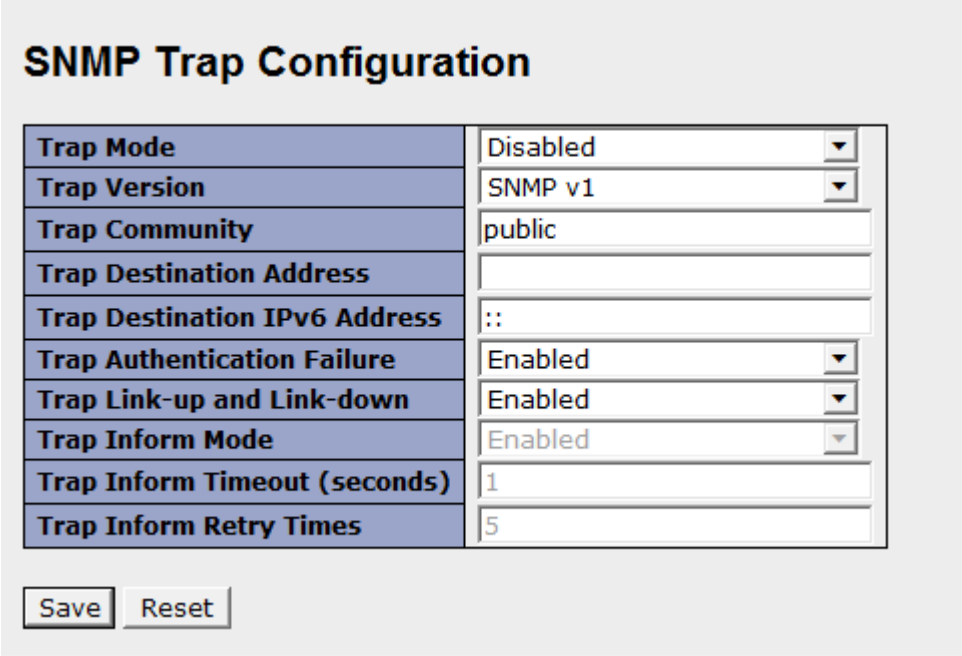


The following table describes the options available.

Option	Description
Mode	The current SNMP mode operation. The two modes are: Enabled: Enable SNMP mode operation. Disabled: Disable SNMP mode operation.
Version	The current SNMP supported version. The three versions are: SNMP v1: Set SNMP supported version 1. SNMP v2c: Set SNMP supported version 2c. SNMP v3: Set SNMP supported version 3.
Read Community	The community read access string for permitting access to the SNMP agent. The allowed string length is from 0 to 255 characters, and the allowed content is the ASCII characters from 33 to 126. The field only applies to SNMPv1 and SNMPv2c. SNMPv3 uses USM for authentication and privacy and the community string associated with the SNMPv3 communities table
Write Community	The community write access string for permitting access to the SNMP agent. The allowed string length is from 0 to 255 characters, and the allowed content is the ASCII characters from 33 to 126. The field only applies to SNMPv1 and SNMPv2c. SNMPv3 uses USM for authentication and privacy and the community string associated with the SNMPv3 communities table
Engine ID	The SNMPv3 engine ID. The string must contain an even number between 10 and 64 hexadecimal digits, but all zero and all 'F' strings are not allowed. Changing the Engine ID will clear all original local users.

6.7.1.2 SNMP Trap configuration

SNMP trap configuration is set using this section.



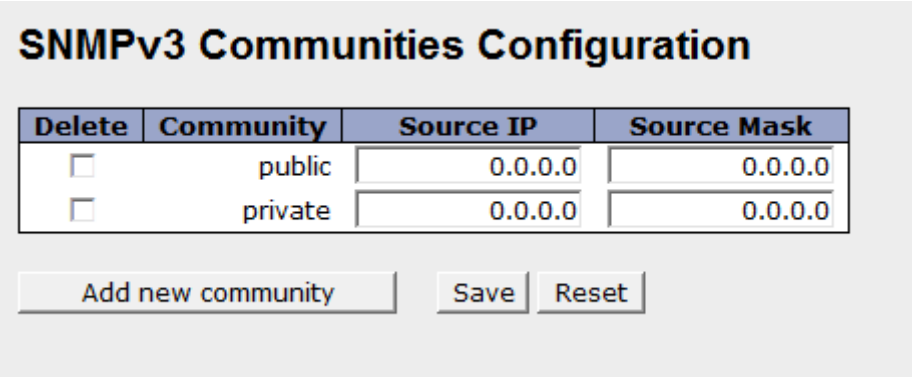
The following table describes the options available.

Option	Description
Trap Mode	The SNMP trap mode operation. The two modes are: Enabled: Enable SNMP trap mode operation. Disabled: Disable SNMP trap mode operation.
Trap Version	The SNMP trap supported version. The three versions are: SNMP v1: Set SNMP trap supported version 1. SNMP v2c: Set SNMP trap supported version 2c. SNMP v3: Set SNMP trap supported version 3.
Trap Community	The community access string for sending SNMP trap packets. The valid string length is 0 to 255 characters, and the permitted content is the ASCII characters from 33 to 126.
Trap Destination Address	The SNMP trap destination address. Trap Destination IPv6 Address
Trap Destination IPv6 Address	The trap destination IPv6 address of the switch. The IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80:215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as an abbreviated way of representing multiple 16-bit groups of continuous zeros; but it can only appear once. It is also

	used a following legally IPv4 address. For example, '::192.1.2.34'.
Trap Authentication Failure	Determines if the SNMP entity is permitted to generate authentication failure traps. The two modes are: Enabled: Enable SNMP trap authentication failure. Disabled: Disable SNMP trap authentication failure.
Trap Link-up and Link-down	Determines the SNMP trap link-up and link-down mode operation. The two modes are: Enabled: Enable SNMP trap link-up and link-down mode operation. Disabled: Disable SNMP trap link-up and link-down mode operation.
Trap Inform Mode	Determines the SNMP trap inform mode operation. The two modes are: Enabled: Enable SNMP trap inform mode operation. Disabled: Disable SNMP trap inform mode operation.
Trap Inform Timeout(seconds)	The SNMP trap inform timeout. The valid range is 0 to 2147.
Trap Inform Retry Times	The SNMP trap inform retry times. The valid range is 0 to 255.
Trap Probe Security Engine ID	Determines the SNMP trap probe security engine ID mode of operation. The two settings are: Enabled: Enable SNMP trap probe security engine ID mode of operation. Disabled: Disable SNMP trap probe security engine ID mode of operation.
Trap Security Engine ID	The SNMP trap security engine ID. SNMPv3 sends traps using USM for authentication and privacy. A unique engine ID for these traps and informs is required. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field will be used. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed.
Trap Security Name	The SNMP trap security name. A unique security name is required when traps and informs are enabled.

6.7.2 SNMP-Communities

The SNMPv3 communities table are configured on this page. Community is the entry index key.

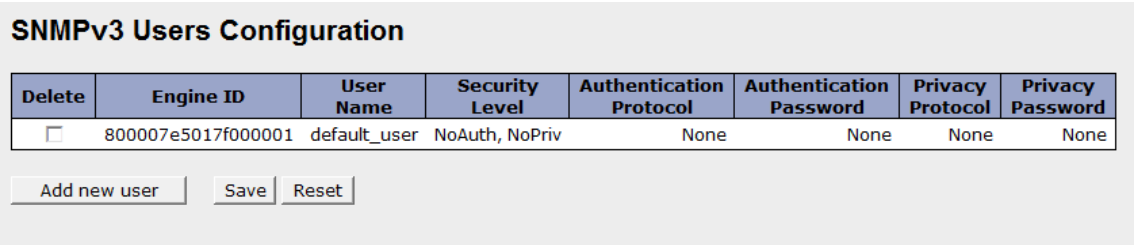


The following table describes the options available.

Option	Description
Delete	Check to delete the entry. It will be deleted at the next save.
Community	The community access string permitting access to the SNMPv3 agent. The valid string length is 1 to 32 characters, and the permitted content is the ASCII characters from 33 to 126.
Source IP	The SNMP access source address.
Source Mask	The SNMP access source address mask.

6.7.3 SNMP-Users

SNMPv3 users are configured on this page. The entry index keys are Engine ID and User Name.

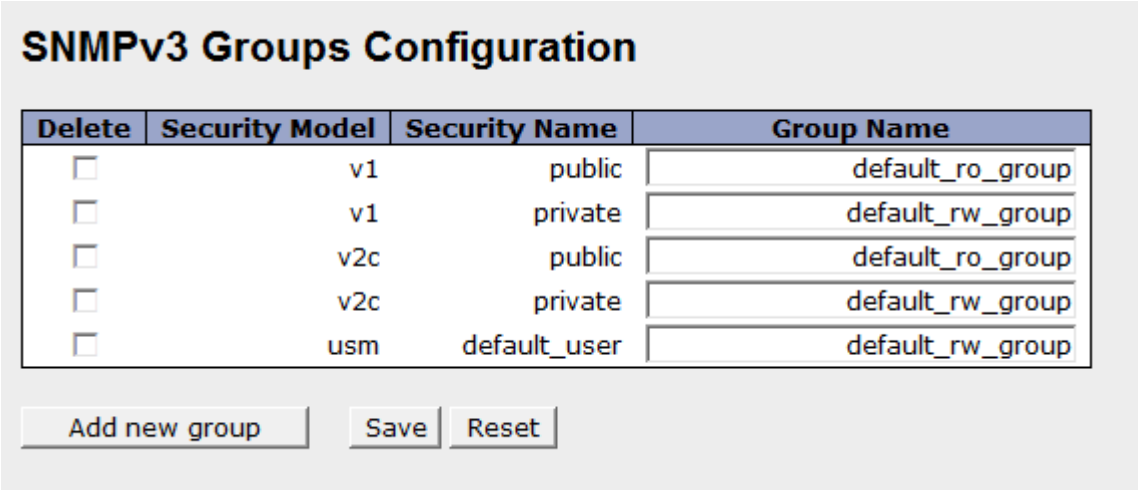


The following table describes the options available.

Option	Description
Delete	Check to delete the entry. It will be deleted at the next save.
Engine ID	An octet string identifying the engine ID to which this entry belongs. The string must contain an even number between 10 and 64 hexadecimal digits, but all zeros and all 'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry keys. In a simple agent, usmUserEngineID is that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if the user engine ID equals the system engine ID then the user is local. Otherwise, the user is remote.
User Name	A string identifying the user name. The valid string length is 1 to 32 characters and the permissible content is limited to the ASCII characters from 33 to 126.
Security Level	The entry's security model. The three security models are: 1. NoAuth, NoPriv: None authentication and no privacy. 2. Auth, NoPriv: Authentication and no privacy. 3. Auth, Priv: Authentication and privacy. The security model cannot be modified if the entry already exists. The security model must be set when the entry is created.
Authentication Protocol	The entry's authentication protocol. The three authentication protocols are: None: No authentication protocol. MD5: MD5 authentication protocol. SHA: SHA authentication protocol. The security model cannot be modified if the entry already exists. The security model must be set when the entry is created.
Authentication Password	A text string identifying the authentication password. For MD5 authentication protocol, the valid string length is 8 to 32 characters. For SHA authentication protocol, the valid string length is 8 to 40. The characters permitted are the ASCII characters from 33 to 126.
Privacy Protocol	The entry's privacy protocol. The two privacy protocols are: None: No privacy protocol. DES: DES authentication protocol.
Privacy Password	A string identifying the privacy password. The allowed string length is from 8 to 32 characters and the characters permitted are the ASCII characters from 33 to 126.

6.7.4 SNMP-Groups

SNMPv3 groups are configured on this page. The entry index keys are Security Model and Security Name.

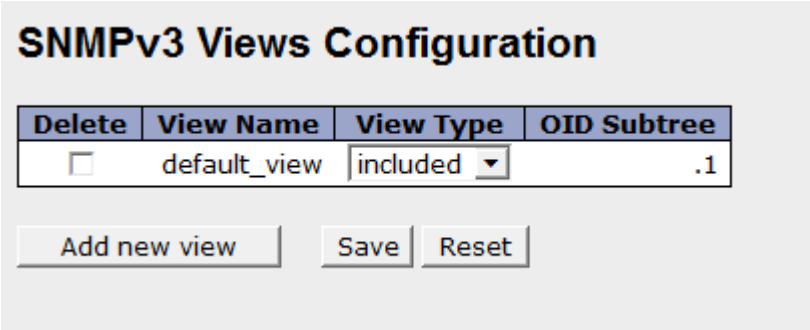


The following table describes the options available.

Option	Description
Delete	Check to delete the entry. It will be deleted at the next save.
Security Model	Indicates the security model to which this entry should belongs. The three security models are: v1: Reserved for SNMPv1. v2c: Reserved for SNMPv2c. usm: User-based Security Model (USM).
Security Name	A string identifying the entry's security name. The valid string length is from 1 to 32 characters, and the ASCII characters from 33 to 126 are permitted.
Group Name	A string identifying the entry's group name. The valid string length is from 1 to 32 characters, and the ASCII characters from 33 to 126 are permitted.

6.7.5 SNMP-Views

SNMPv3 views are configured on this page. The entry index keys are View Name and OID Subtree.

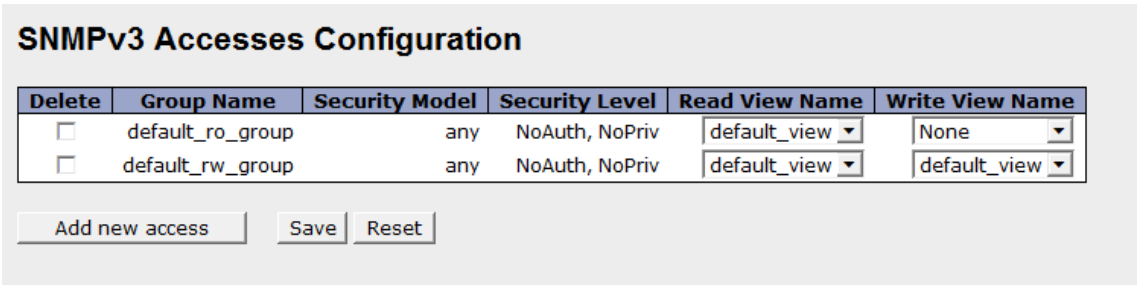


The following table describes the options available.

Option	Description
Delete	Check to delete the entry. It will be deleted at the next save.
View Name	A string identifying the entry's view name. The valid string length is from 1 to 32 characters, and the ASCII characters from 33 to 126 are permitted.
View Type	The view type for this entry. The two view types are: included: This view subtree is included. excluded: This view subtree is excluded. If a view entry's view type is 'excluded', there should be another view entry whose view type is 'included' and its OID subtree should overstep the 'excluded' view entry.
OID Subtree	The OID defining the root of the subtree of the named view. The valid OID length is from 1 to 128 characters. The permitted content is digital numbers or asterisks (*).

6.7.6 SNMP-Accesses

SNMPv3 access table are modified here. The entry index keys are Group Name, Security Model and Security Level.



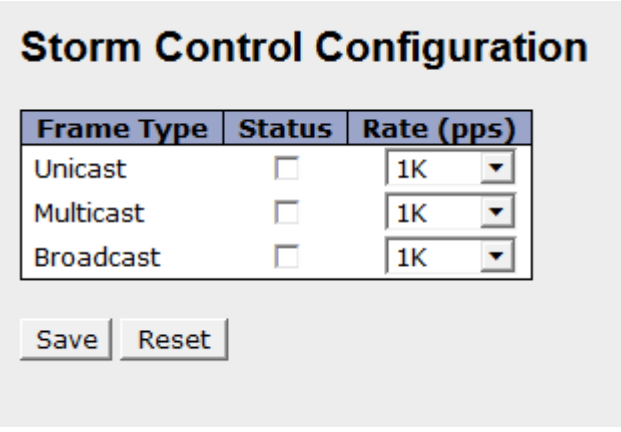
The following table describes the options available.

Option	Description
Delete	Check to delete the entry. It will be deleted at the next save.
Group Name	A string identifying the group name. The valid string length is from 1 to 32 characters, and the ASCII characters from 33 to 126 are permitted.
Security Model	The entry's security model that this entry should belong to. The four options are: any: Any security model is accepted. (v1|v2c|usm). v1: Reserved for SNMPv1. v2c: Reserved for SNMPv2c. usm: User-based Security Model (USM).
Security Level	The entry's security level. The three security leves are: NoAuth, NoPriv: No authentication and no privacy. Auth, NoPriv: Authentication and no privacy. Auth, Priv: Authentication and privacy.
Read View Name	The name of the MIB view defining the MIB objects for which a request may ask for the current values. The valid string length is from 1 to 32 characters, and ASCII characters from 33 to 126 are permitted.
Write View Name	The name of the MIB view defining the MIB objects for which a request may set new values. The valid string length is from 1 to 32 characters, and ASCII characters from 33 to 126 are permitted.

6.8 Traffic Prioritization

6.8.1 Storm Control

Storm control for the switch is configured on this page.



You can set Unicast storm rate control, Multicast storm rate control and Broadcast storm rate control. These only affect flooded frames, i.e. frames with a VLAN ID-DMAC pair not present on the MAC Address table. The rate is 2^n, where n is equal to or less than 15, or "No Limit". The unit of the rate can be either pps (packets per second) or kpps (kilopackets per second). The configuration shows the permitted packet rate for unicast, multicast, or broadcast traffic across the switch.

Note: Frames, which are sent to the CPU of the switch are always limited to approximately 4 kpps. For example, broadcasts in the management VLAN are limited to this rate. The management VLAN is configured on the IP setup page.

The following table describes the options available.

Option	Description
Frame Type	The settings in a particular row apply to the frame type listed here: unicast, multicast, or broadcast.
Status	Enable or disable the storm control status for the given frame type.
Rate	The rate unit is packet per second (pps), configure the rate as 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, or 1024K. The 1 kpps is actually 1002.1 pps.

6.8.2 Port QoS Configuration

This page allows you to configure QoS settings for each port.

Frames can be classified by 4 different QoS classes: Low, Normal, Medium, and High.

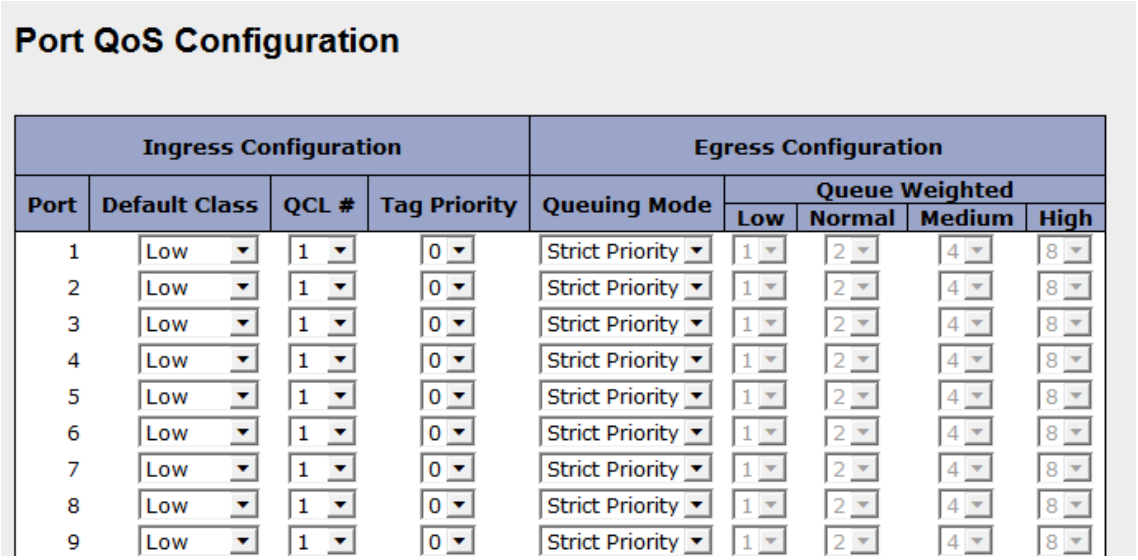
The classification is controlled by a QCL that is assigned to each port.

A QCL consists of an ordered list of up to 12 QCEs.

Each QCE is used to classify certain frames to a specific QoS class.

This classification can be based on parameters such as VLAN ID, UDP/TCP port, IPv4/IPv6 DSCP or Tag Priority.

Frames not matching any of the QCEs will be classified as the port's default QoS class.


Port QoS Configuration
Ingress Configuration
Egress Configuration
Port
Default Class
QCL #
Tag Priority
Queuing Mode
Queue Weighted
Low
Normal
Medium
High
1 Low 1 0 Strict Priority 1 2 4 8
2 Low 1 0 Strict Priority 1 2 4 8
3 Low 1 0 Strict Priority 1 2 4 8
4 Low 1 0 Strict Priority 1 2 4 8
5 Low 1 0 Strict Priority 1 2 4 8
6 Low 1 0 Strict Priority 1 2 4 8
7 Low 1 0 Strict Priority 1 2 4 8
8 Low 1 0 Strict Priority 1 2 4 8
9 Low 1 0 Strict Priority 1 2 4 8

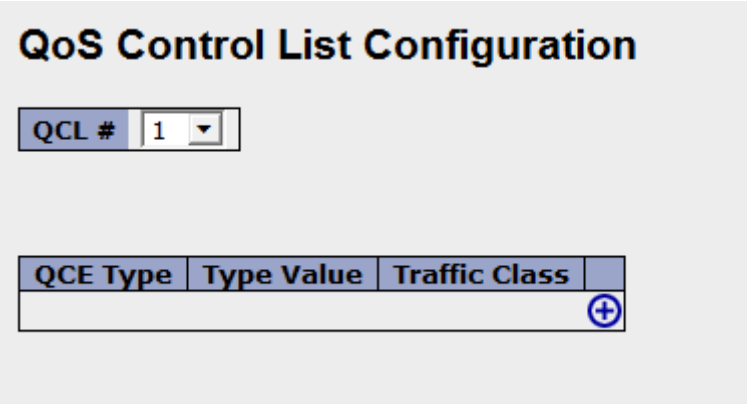
The following table describes the options available.

Option	Description
Port	A check box is provided for each private VLAN port. When checked, port isolation is enabled for that port. When unchecked, port isolation is disabled for that port. Port isolation is disabled for all ports by default.
Default Class	Configure the default QoS class for the port. This is the QoS class for frames that do not match any of the QCEs in the QCL.
QCL#	Select which QCL used bythe port.
Tag Priority	Select the priority for this port when adding a Tag to the untagged frames.
Queuing Mode	Select the Queuing mode for this port.
Queue Weighted	Set the Queue weighting, (Low=Normal, Medium=High), if the "Queuing Mode" is "Weighted".

6.8.3 QoS Control List Configuration

This page lists the QCEs for a given QCL. Frames can be classified by 4 different QoS classes: Low, Normal, Medium, and High.

The classification is controlled by a QoS assigned to each port. A QCL consists of an ordered list of up to 12 QCEs. Each QCE can be used to classify certain frames to a specific QoS class. This classification can be based on parameters such as VLAN ID, UDP/TCP port, IPv4/IPv6 DSCP or Tag Priority. Frames not matching any of the QCEs are classified as the default QoS Class for the port.



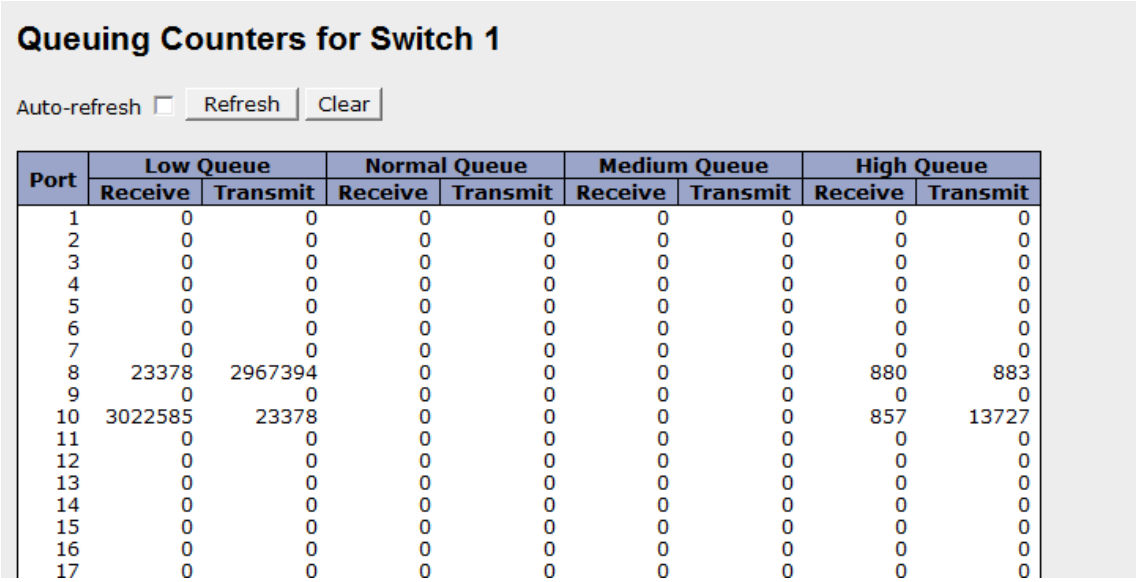
The following table describes the options available.

Option	Description
QCL#	Select a QCL to display a table that lists all the QCEs for that particular QCL.
QCE Tyep	Specifies which frame field the QCE processes to determine the QoS class of the frame. The following QCE types are supported: Ethernet Type: If the frame is tagged, this is the Ethernet Type that follows the tag header. VLAN ID: VLAN ID. Only applicable if the frame is VLAN-tagged. TCP/UDP Port: IPv4 TCP/UDP source/destination port. DSCP: IPv4 and IPv6 DSCP. ToS: The three-precedence bit in the ToS byte of the IPv4/IPv6 header. Also known as DS field. Tag Priority: User Priority. Only applicable if the frame is VLAN-tagged or priority-tagged.
Type Value	The value according to its QCE type: Ethernet Type: The Ethernet Type value. VLAN ID: The VLAN ID. TCP/UDP Port: The TCP/UDP port range. DSCP: The IPv4/IPv6 DSCP value.
Traffic Class	The QoS class associated with the QCE.
Modification Buttons	You can modify each QCE in the table using the following buttons: (+) : Inserts a new QCE before the current row. (e) : Edits the QCE.

	(^) : Moves the QCE up the list. (v) : Moves the QCE down the list. (x) : Deletes the QCE. (+) : The lowest plus sign adds a new entry at the bottom of the QCL list.

6.8.4 Queuing Counters

This page provides statistics for the different queues for all switch ports.



Queuing Counters for Switch 1

Auto-refresh ☐ Refresh Clear

Port	Low Queue		Normal Queue		Medium Queue		High Queue	
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	23378	2967394	0	0	0	0	880	883
9	0	0	0	0	0	0	0	0
10	3022585	23378	0	0	0	0	857	13727
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0

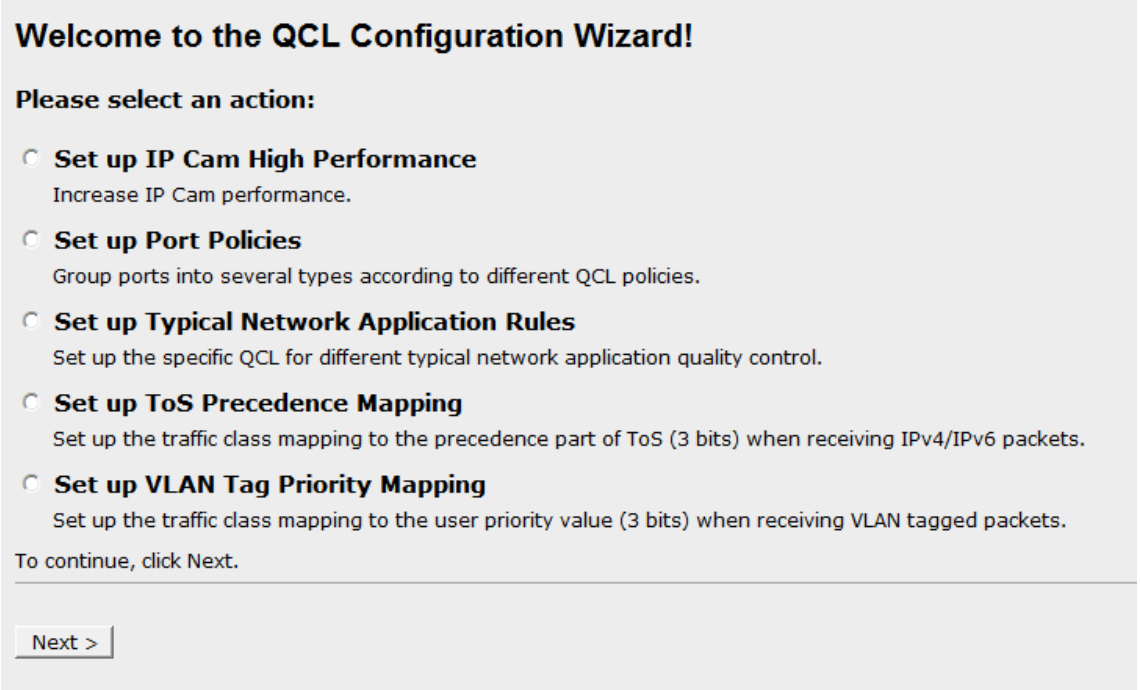
The following table describes the options available.

Option	Description
Port	The logical port for the settings contained in the same row.
Low Queue	There are 4 QoS queues per port with strict or weighted queuing scheduling. This is the lowest priority queue.
Normal Queue	This is the normal priority queue of the 4 QoS queues. It has higher priority than the "Low Queue".
Medium Queue	This is the medium priority queue of the 4 QoS queues. It has higher priority than the "Normal Queue".
High Queue	This is the highest priority queue of the 4 QoS queues
Receive/Transmit	The number of received and transmitted packets per port.

Refresh	Refreshes the page immediately
Clear	Clears the counters for all ports
Auto Refresh	Refreshes the page at regular intervals

6.8.5 Wizard

The wizard helps you set up a QCL quickly.


Welcome to the QCL Configuration Wizard!
Please select an action:
Set up IP Cam High Performance
Increase IP Cam performance.
Set up Port Policies
Group ports into several types according to different QCL policies.
Set up Typical Network Application Rules
Set up the specific QCL for different typical network application quality control.
Set up ToS Precedence Mapping
Set up the traffic class mapping to the precedence part of ToS (3 bits) when receiving IPv4/IPv6 packets.
Set up VLAN Tag Priority Mapping
Set up the traffic class mapping to the user priority value (3 bits) when receiving VLAN tagged packets.
To continue, click Next.
Next >

The following table describes the options available.

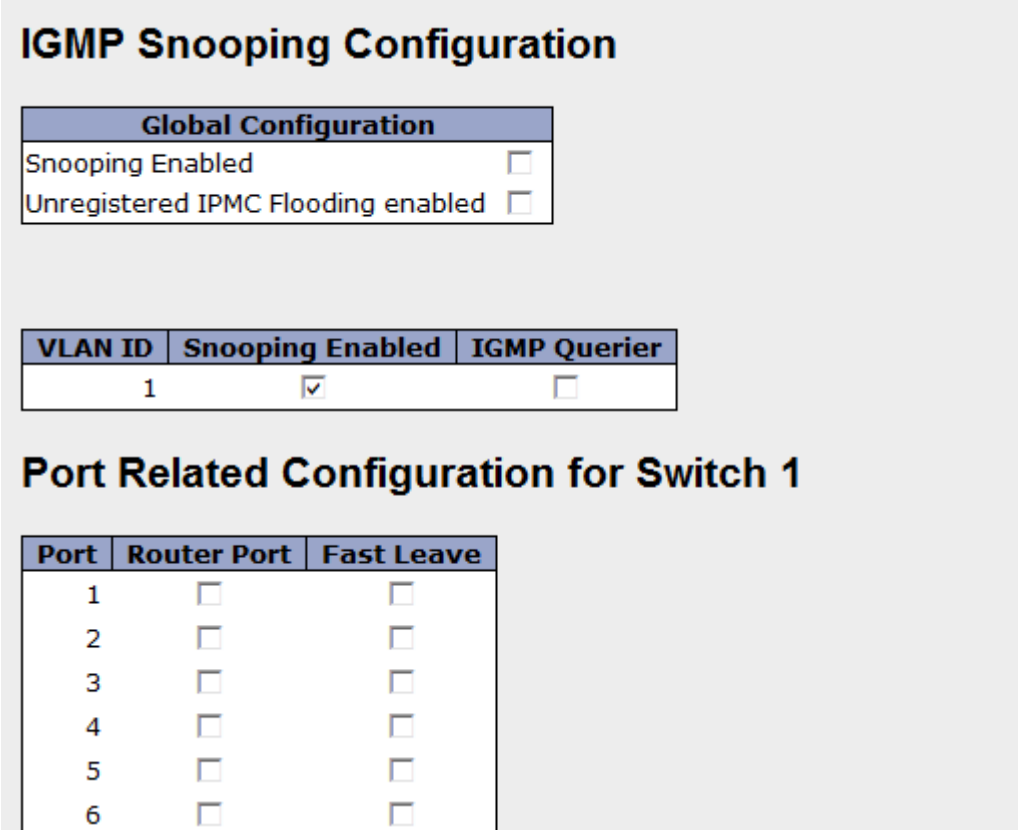
Option	Description
Set up **Port Policies**	Group ports into several types according to QCL policy.
Set up Typical Network Application Rules	Set up the specific QCL for different network application quality control.
Set up ToS Precedence Mapping	Set up the traffic class mapping to the precedence part of ToS (3 bits) when receiving IPv4/IPv6 packets.
Set up VLAN Tag Priority Mapping	Set up the traffic class mapping to the User Priority value (3 bits) when receiving VLAN tagged packets.

6.9 Multicast

6.9.1 IGMP Snooping

6.9.1.1 IGMP Configuration

This page is used to configure IGMP Snooping.



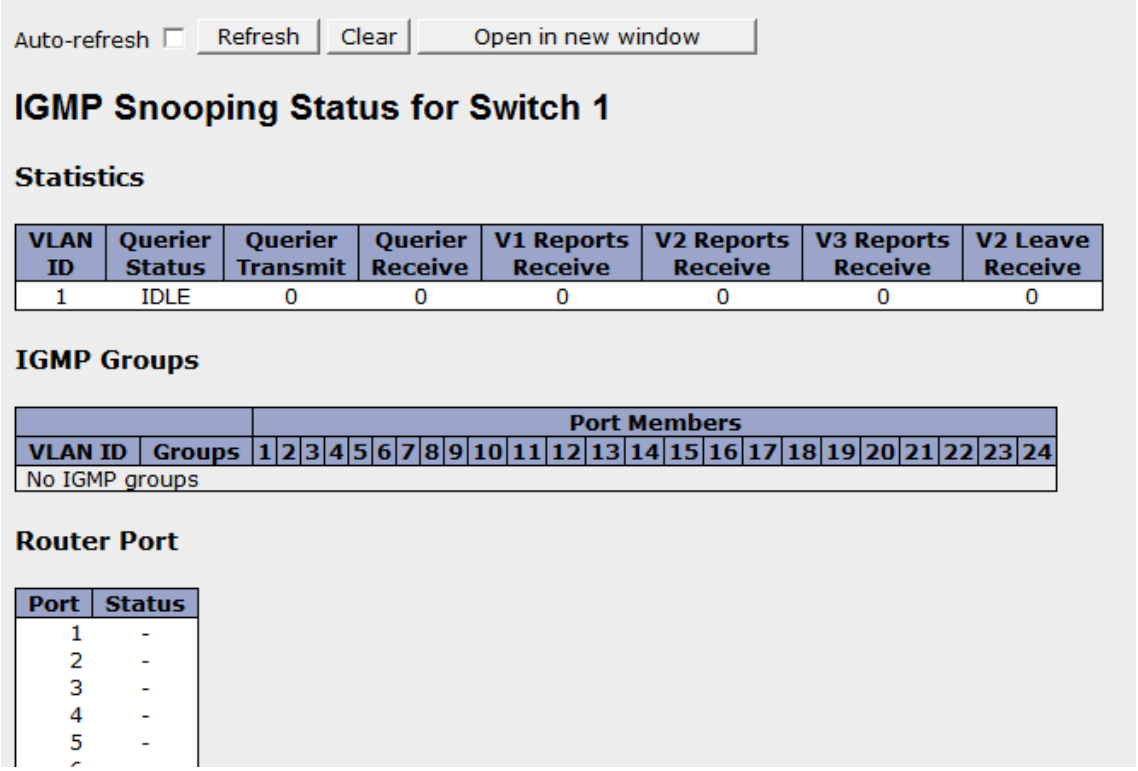
The following table describes the options available.

Label	Description
Snooping Enabled	Enable Global IGMP Snooping.
Unregistered IPMC Flooding enabled	Enable unregistered IPMC traffic flooding.
VLAN ID	The entry's VLAN ID.
IGMP Snooping Enabled	Enable the per-VLAN IGMP Snooping.
IGMP Querier	Enable the IGMP Querier for the VLAN. The Querier will send out if no Query is received in 255 seconds after IGMP Querier is Enabled. Each Query's interval is 125 second, and it will stop acting as an IGMP Querier if it receives any Query from other devices.

Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or the IGMP querier. If an aggregation member port is selected as a router port, the entire aggregation will act as a router port.
Fast Leave	Enable fast leave on the port.

6.9.2 IGMP Snooping Status

IGMP Snooping Status is set up using this page.


Auto-refresh
Refresh
Clear
Open in new window
IGMP Snooping Status for Switch 1
Statistics
VLAN ID | Querier Status | Querier Transmit | Querier Receive | V1 Reports Receive | V2 Reports Receive | V3 Reports Receive | V2 Leave Receive
1 | IDLE | 0 | 0 | 0 | 0 | 0 | 0
IGMP Groups
Port Members
VLAN ID | Groups | 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
No IGMP groups
Router Port
Port | Status
1 -
2 -
3 -
4 -
5 -

The following table describes the options available.

Option	Description
VLAN ID	The VLAN ID.
Groups	The present IGMP groups. There are a maximum of 128 groups for each VLAN.
Port Members	The ports that are members of the entry.
Querier Status	Shows Querier status as "ACTIVE" or "IDLE".
Querier Receive	The number of Transmitted Queriers.

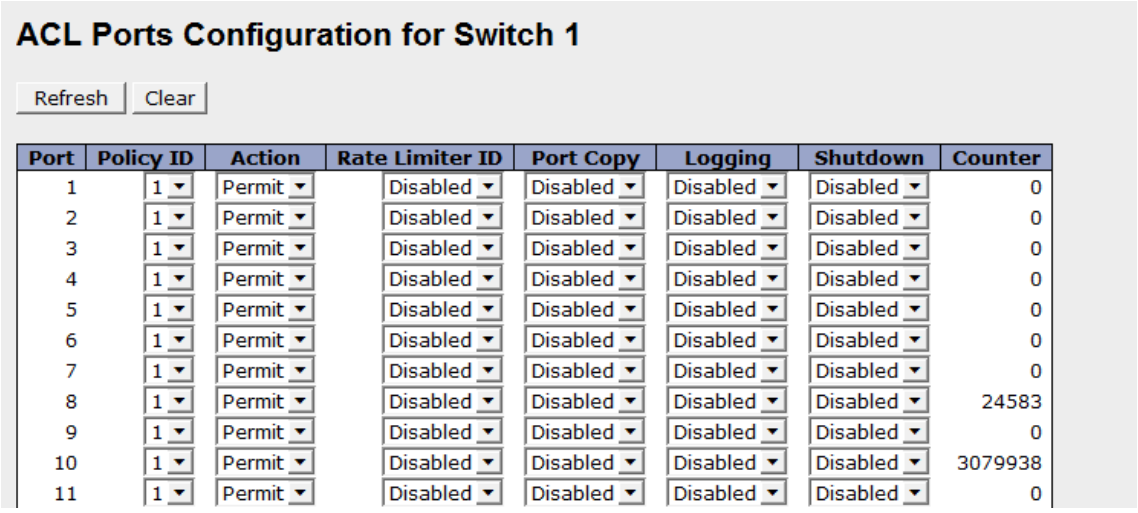
V1 Reports Receive	The number of Received V1 Reports.
V2 Reports Receive	The number of Received V2 Reports.
V3 Reports Receive	The number of Received V3 Reports.
V2 Leave Receive	The number of Received V2 Leaves.
Refresh	Click to refresh the page.
Clear	Clears all Statistics counters.
Auto Refresh	Check this box to enable the automatic refresh of the page at regular intervals.

6.10 Security

6.10.1 ACL

6.10.1.1 ACL port configuration

You can configure the ACL parameters of the ACE of each switch port using this page. These parameters will affect frames received on a port unless the frame matches a specific ACE.

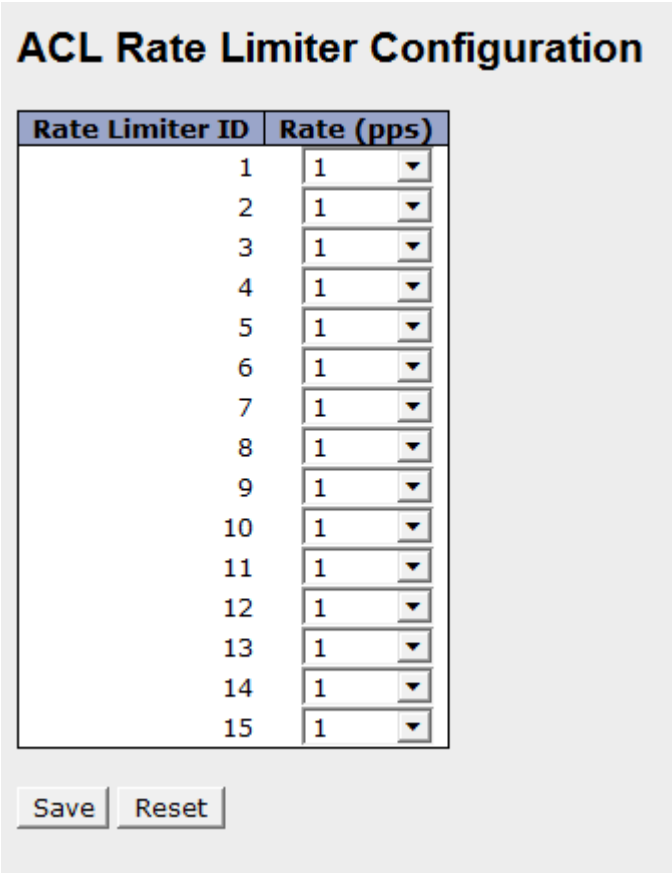

ACL Ports Configuration for Switch 1
Refresh
Clear
Port
Policy ID
Action
Rate Limiter ID
Port Copy
Logging
Shutdown
Counter
1 1 Permit Disabled Disabled Disabled Disabled 0
2 1 Permit Disabled Disabled Disabled Disabled 0
3 1 Permit Disabled Disabled Disabled Disabled 0
4 1 Permit Disabled Disabled Disabled Disabled 0
5 1 Permit Disabled Disabled Disabled Disabled 0
6 1 Permit Disabled Disabled Disabled Disabled 0
7 1 Permit Disabled Disabled Disabled Disabled 0
8 1 Permit Disabled Disabled Disabled Disabled 24583
9 1 Permit Disabled Disabled Disabled Disabled 0
10 1 Permit Disabled Disabled Disabled Disabled 3079938
11 1 Permit Disabled Disabled Disabled Disabled 0

The following table describes the options available.

Option	Description
Port	The port settings.
Policy ID	Select the policy that applies to this port. The permitted values are 1 through 8. The default value is 1.
Action	Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".
Rate Limiter ID	Select which rate limiter applies to this port. The permitted values are Disabled or the numerical values 1 through 15. The default value is "Disabled".
Port Copy	Select which port frames are copied. The allowed values are Disabled or a specific port number. The default value is "Disabled".
Logging	Specify the logging operation of this port. The two options are: Enabled: Frames received on the port are stored in the System Log. Disabled: Frames received on the port are not logged. The default value is "Disabled". Please note that the System Log's memory size and logging rate are limited.
Shutdown	Specify the shut down operation of this port. The two options are: Enabled: If a frame is received on the port, the port will be disabled. Disabled: Port shut down is disabled. The default value is "Disabled".
Counter	Counts the number of frames that match this ACE.

6.10.1.2 ACL Rate Limiter

The ACL Rate limiter is configured using this page.



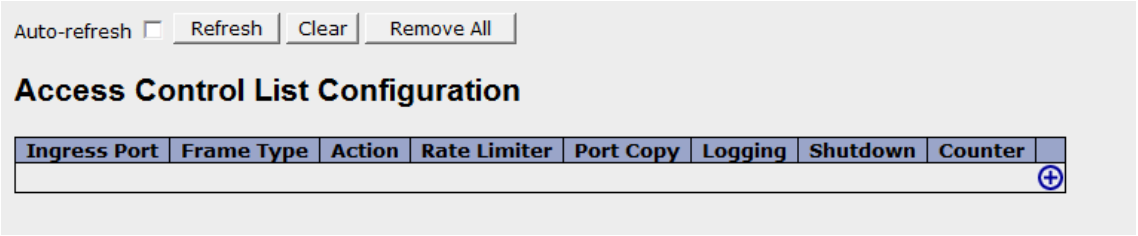
The following table describes the options available.

Option	Description
Rate Limiter ID	Use this to rate limiter ID
Rate	The rate unit is packet per second (pps), configure the rate as 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, or 1024K. Note: the 1 kpps is actually 1024 pps.

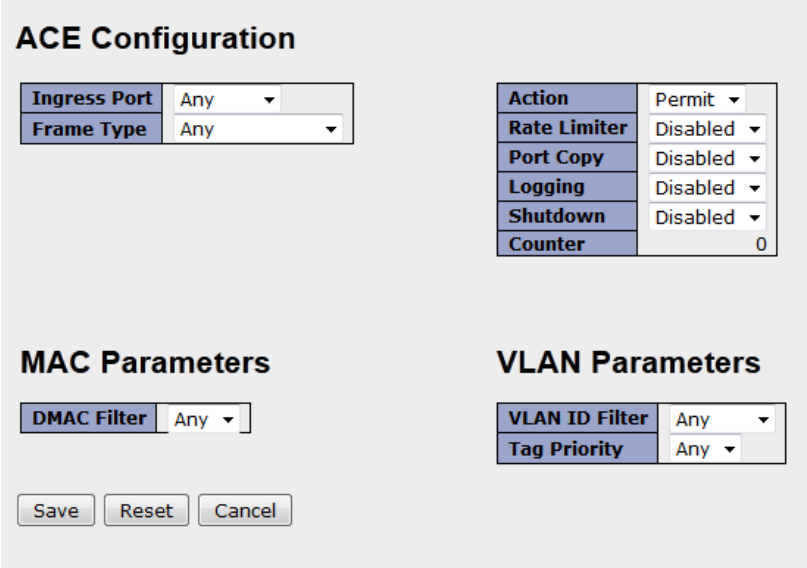
6.10.1.3 Access Control List Configuration

The Access Control List is configured using this page.

This page shows the Access Control List (ACL) which is made up of the ACEs defined for this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 128.



Click on the lowest plus sign to add a new ACE to the list.



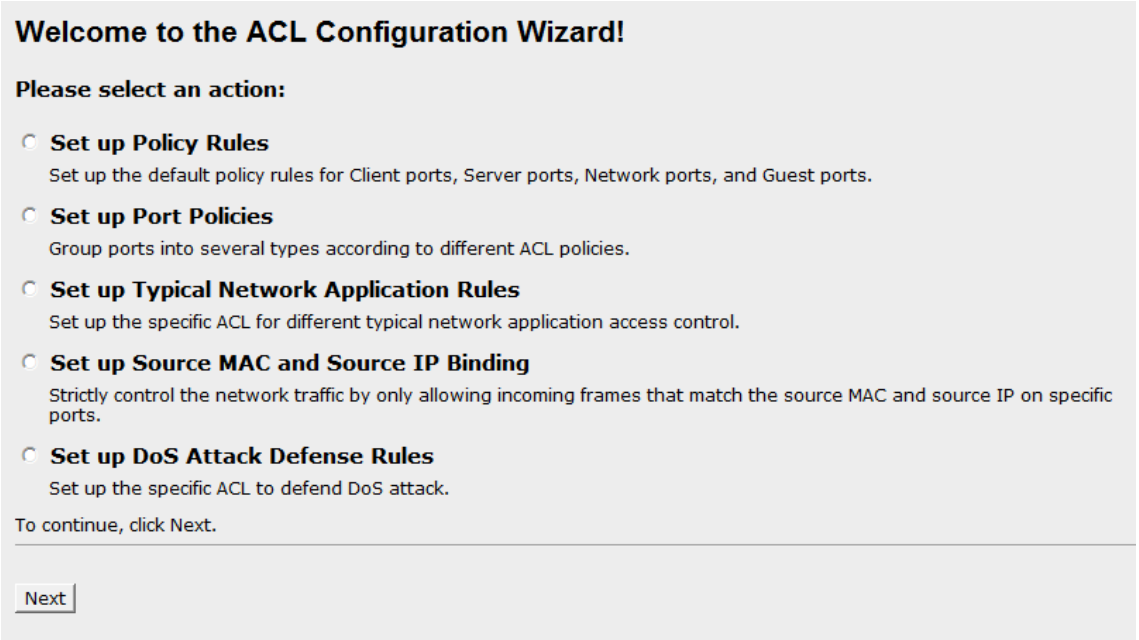
The following table describes the options available.

Option	Description
Ingress port	Indicates the ingress port of the ACE. Any: The ACE will match any ingress port. Policy: The ACE will match ingress ports with a specific policy. Port: The ACE will match a specific ingress port.
QCE Type	Indicates the frame type of the ACE. Any: ACE will match any frame type. EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. ARP: The ACE will match ARP/RARP frames. IPv4: The ACE will match all IPv4 frames. IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol. IPv4/UDP: The ACE will match IPv4 frames with UDP protocol. IPv4/TCP: The ACE will match IPv4 frames with TCP protocol. IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.

Action	Indicates the forwarding action of the ACE. Permit: Frames matching the ACE may be forwarded and learned. Deny: Frames matching the ACE are dropped.
Rate Limiter	Indicates the rate limiter number of the ACE. The allowed range is 1 to 15. When Disabled is displayed, the rate limiter operation is disabled.
Port Copy	Indicates the port copy operation of the ACE. Frames matching the ACE are copied to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port copy operation is disabled.
Logging	Indicates the logging operation of the ACE. Possible values are: Enabled: Frames matching the ACE are stored in the System Log. Disabled: Frames matching the ACE are not logged. Please note that the System Log memory size and logging rate is limited.
Shutdown	Indicates the port shut down operation of the ACE. Possible values are: Enabled: If a frame matches the ACE, the ingress port will be disabled. Disabled: Port shut down is disabled for the ACE
Counter	The counter indicates the number of times the ACE was hit by a frame.
Modification Buttons	You can modify each ACE in the table using the following buttons: (+) : Inserts a new ACE before the current row. (e) : Edits the ACE. (^) : Moves the ACE up the list. (v) : Moves the ACE down the list. (x) : Deletes the ACE. (+) : The lowest plus sign adds a new entry at the bottom of the ACE listing
Auto Refresh	Refreshes the page automatically
Refresh	Refreshes the page
Clear	Clears all the counters
Remove all	Removes all of the ACEs

6.10.1.4 ACL Wizard

This Wizard helps you configure ACL quickly.


Welcome to the ACL Configuration Wizard!
Please select an action:
Set up Policy Rules
Set up the default policy rules for Client ports, Server ports, Network ports, and Guest ports.
Set up Port Policies
Group ports into several types according to different ACL policies.
Set up Typical Network Application Rules
Set up the specific ACL for different typical network application access control.
Set up Source MAC and Source IP Binding
Strictly control the network traffic by only allowing incoming frames that match the source MAC and source IP on specific ports.
Set up DoS Attack Defense Rules
Set up the specific ACL to defend DoS attack.
To continue, click Next.
Next

Option	Description
Set up Policy Rules	Set up the default policy rules for Client ports, Server ports, Network ports and Guest ports.
Set up Port Policies	Group ports into several types according to different ACL policies.
Set up Typical Network Application Rules	Set up the specific ACL for different typical network application access control.
Set up Source MAC & Source IP binding rules	Strictly control the network traffic by only allowing incoming frames that match the source IP and source MAC on specific port.
Set up DoS Attack Defence Rules	Set up the specific ACL to prevent DoS attacks.
Next	Move on to the next step

6.10.2 802.1x

This page allows you to configure the IEEE 802.1x and MAC-based authentication system and port settings.

The IEEE 802.1x standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the RADIUS servers, determine whether the user is allowed access to the network. The RADIUS servers are configured on the Authentication configuration page.

MAC-based authentication allows for authentication of more than one user on the same

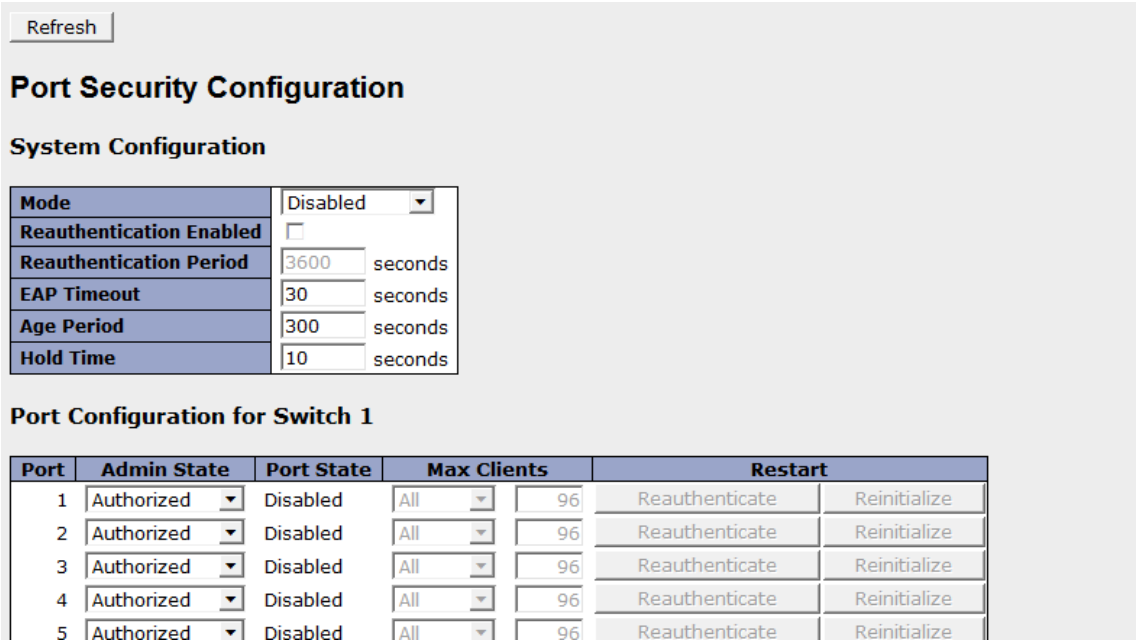
port, and doesn't require the user to have special 802.1x software installed on his system. The switch uses the user's MAC address to authenticate against the backend server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1x authentication.

The 802.1X and MAC-Based Authentication configuration consists of two sections, a system-wide and individual port configuration.

6.10.2.1 Configuration

System Configuration

This section enables you to set up the System security configurations.



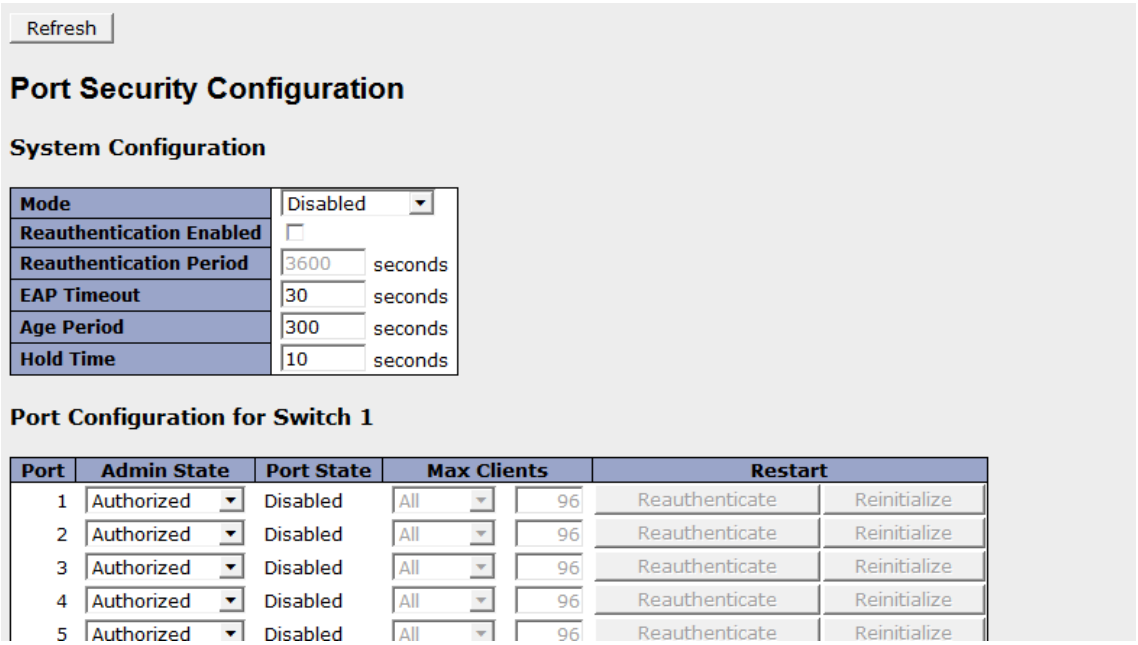
The following table describes the options available.

Option	Description
Mode	Indicates if 802.1X and MAC-based authentication is globally enabled or disabled on the switch. If globally disabled, all ports are allowed to forward of frames.
Re-authentication enabled	If checked, clients are re-authenticated after the interval specified by the Re-authentication Period. Re-authentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port. For MAC-based ports, re-authentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port.

Re-authentication Period	The time in seconds after which a connected client must be re-authenticated. Valid values are in the range 1 to 3600 seconds.
EAP Timeout	The time the switch waits for the supplicant response before retransmitting a packet. Range 1 to 255 seconds. This has no effect for MAC-based ports.
Age Period	This applies to MAC-based authentication, only. The Age Period can be set to 10 and 1000000 seconds.
Hold Time	This setting applies to ports running MAC-based authentication, only. The Hold Time determines the time after an EAP Failure indication or RADIUS timeout that a client is not allowed access. The Hold Time can be set to 10 and 1000000 seconds.

Port Configuration

This section enables you to set up the Port security configurations.



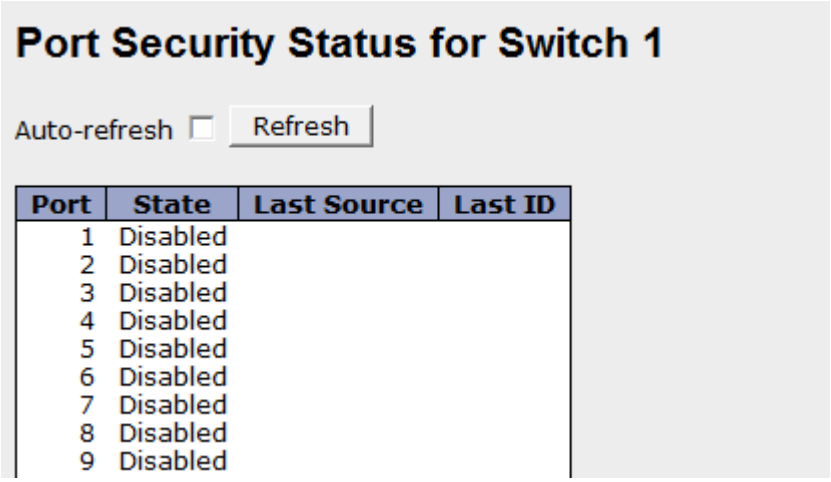
The following table describes the options available.

Option	Description
Port	The port number for the configuration
Admin State	Sets the authentication mode to one of the following options (only used when 802.1X or MAC-based authentication is globally enabled. **Auto:** Requires an 802.1X-aware client (supplicant) to be authorized by the authentication server. **Authorized:** Forces the port to grant access to all clients,

	802.1X-aware or not. **Unauthorized:** Forces the port to deny access to all clients, 802.1X-aware or not. **MAC-Based:** Enables MAC-based authentication on the port. The switch doesn't transmit or accept EAPOL frames on the port. Flooded frames and broadcast traffic will be transmitted on the port, whether or not clients are authenticated on the port, whereas unicast traffic against an unsuccessfully authenticated client will be dropped. Clients that are not (yet) successfully authenticated will not be allowed to transmit frames of any kind.
Port State	The current state of the port. **Disabled:** 802.1X and MAC-based authentication is globally disabled. **Link Down:** 802.1X or MAC-based authentication is enabled, but there is no link on the port. **Authorized:** The port is authorized. **Unauthorized:** The port is unauthorized. **X Auth/Y Unauth:** X clients are currently authorized and Y are unauthorized.
Max Clients	Applies to ports running MAC-based authentication, only. The maximum number of clients allowed on a given port can be configured. There is a maximum of 112 across the whole switch.
Restart	**Reauthenticate:** Schedules a re-authentication with port based authentication whenever the quiet-period of the port runs out. For MAC-based authentication, reauthentication will be attempted immediately. **Reinitialize:** Forces a re-initialization of the port/clients and thereby a re-authentication immediately. The port/clients will transfer to the unauthorized state while the re-authentication is taking place.
Refresh	Refreshes the page
Save	Saves the changes
Reset	Reverts to previously saved changes

6.10.2.2 Port Security Status

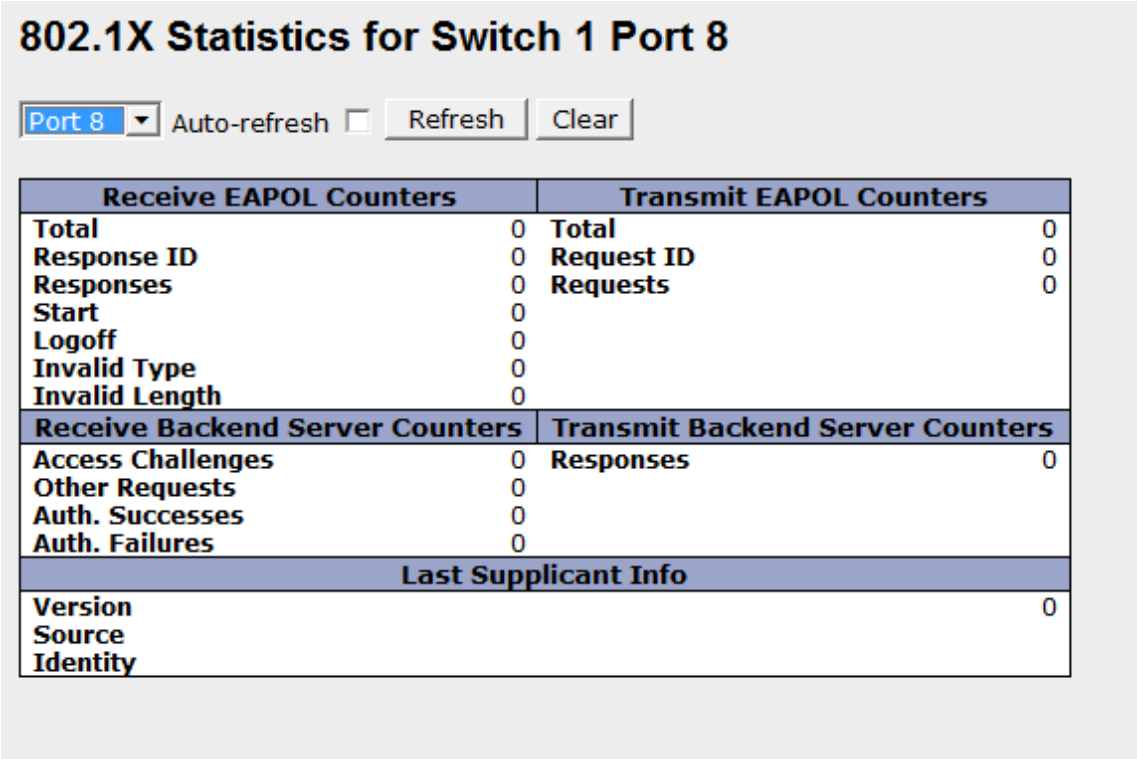
This page provides an overview of the current 802.1x port states.



Option	Description
Port	Switch port number
Port State	The current state of the port.
Last Source	The source MAC address carried in the most recently received EAPOL frame for port-based authentication, and the most recently received frame from a new client for MAC-based authentication.
Last ID	The user name (supplicant identity) carried in the most recently received Resp/ID EAPOL frame for port-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.
Refresh	Refreshes the page
Auto Refresh	Check this box to enable an automatic refresh of the page at regular intervals.

6.10.2.3 802.1x Statistics

This page provides detailed 802.1x statistics for a specific switch port running port-based authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics, only. Use the port select box to select which port details to be displayed.



The following table describes the options available.

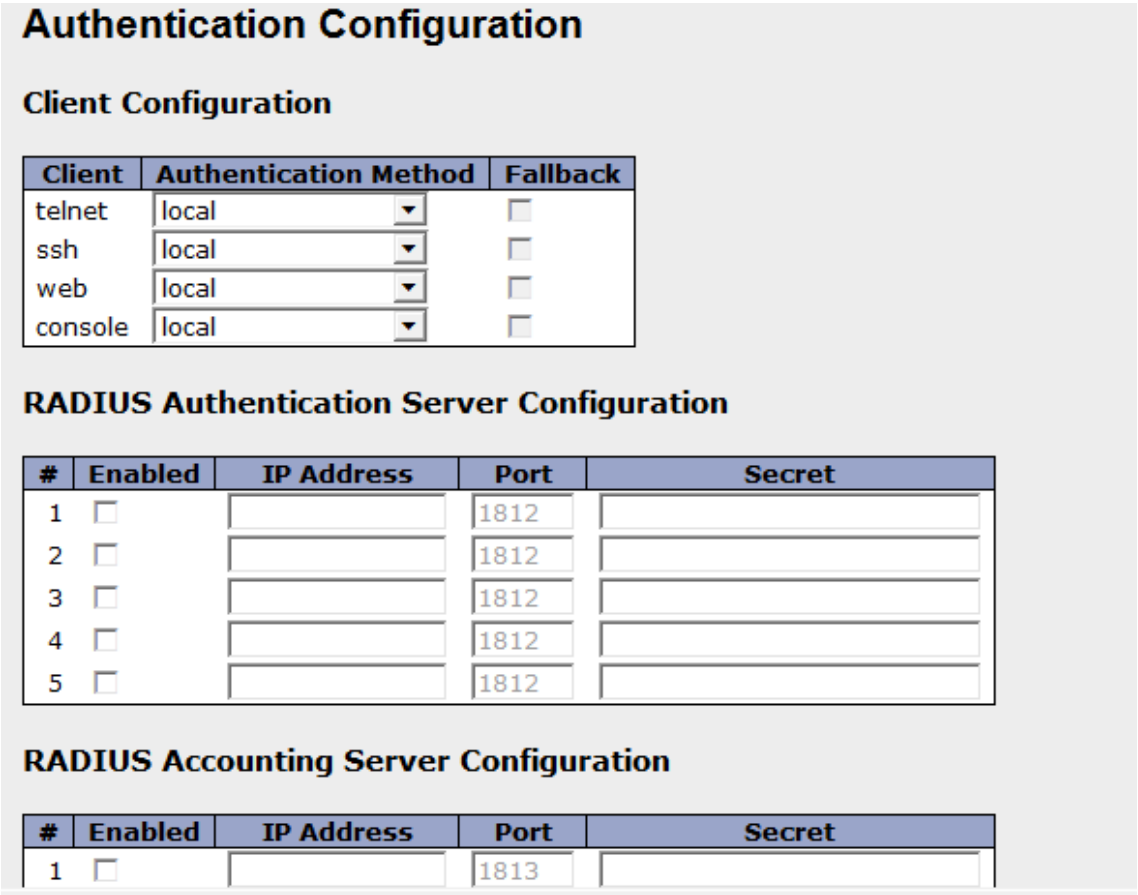
Option	Description
Receive Total	The number of valid EAPOL frames of any type that have been received by the switch.
Receive Response ID	The number of valid EAP Resp/ID frames that have been received by the switch.
Receive Responses	The number of valid EAPOL response frames (other than Resp/ID frames) that have been received by the switch.
Receive Start	The number of EAPOL Start frames that have been received by the switch.
Receive Logoff	The number of valid EAPOL logoff frames that have been received by the switch.
Receive Invalid Type	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.
Receive Invalid Length	The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.
Transmit Total	The number of EAPOL frames of any type that have been transmitted by the switch.
Transmit Request ID	The number of EAP initial request frames that have been

	transmitted by the switch.
Transmit Requests	The number of valid EAP Request frames (other than initial request frames) that have been transmitted by the switch.
Receive Access Challenges	**Port-based**: Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch. **MAC-based**: Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).
Receive Other Requests	**Port-based**: Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method. **MAC-based**: Not applicable
Receive Authentication Requests	**Port- and MAC-based**: Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server.
Receive Authentication Failures	**Port- and MAC-based**: Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.
Transmit Responses	**Port-based:** Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted. **MAC-based:** Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.
Version	**Port-based**: The protocol version number carried in the most recently received EAPOL frame. **MAC-based**: Not applicable.
Source	**Port-based**:

	The source MAC address carried in the most recently received EAPOL frame. **MAC-based**: Not applicable.
Identity	**Port-based**: The user name (supplicant identity) carried in the most recently received Resp/ID EAPOL frame. **MAC-based**: The MAC address of the last client that attempted to authenticate (left-most table), or the MAC address of the currently selected client (right-most table).
Refresh	Refreshes the page immediately
Clear	Clears the counters for the selected port

6.10.2.4 Authentication

This page allows you to configure how an administrator is authenticated when he logs into the switch.



Client Configuration

The following table describes the options available.

Option	Description
Client	The Client for this configuration
Authentication Method	None: Authentication disabled and login is not possible Local: Use the local user database on the switch for authentication Radius: use a remote RADIUS server for authentication
Fallback	Enable fallback to local authentication if authentication method is set to RADIUS

RADIUS Authentication Server Configuration

There is one row for each RADIUS Authentication Server.

The following table describes the options available.

Option	Description
Enable	Check to enable the RADIUS Authentication Server
IP Address	IP address of the RADIUS Authentication Server in dotted decimal notation
Port	THE UDP port to use on the RADIUS Authentication Server. If the port is set to 0 (zero) the default port (1812) is used on the RADIUS Authentication Server
Secret	The password (up to 29 characters) shared between the RADIUS Authentication Server and the switch

RADIUS Accounting Server Configuration

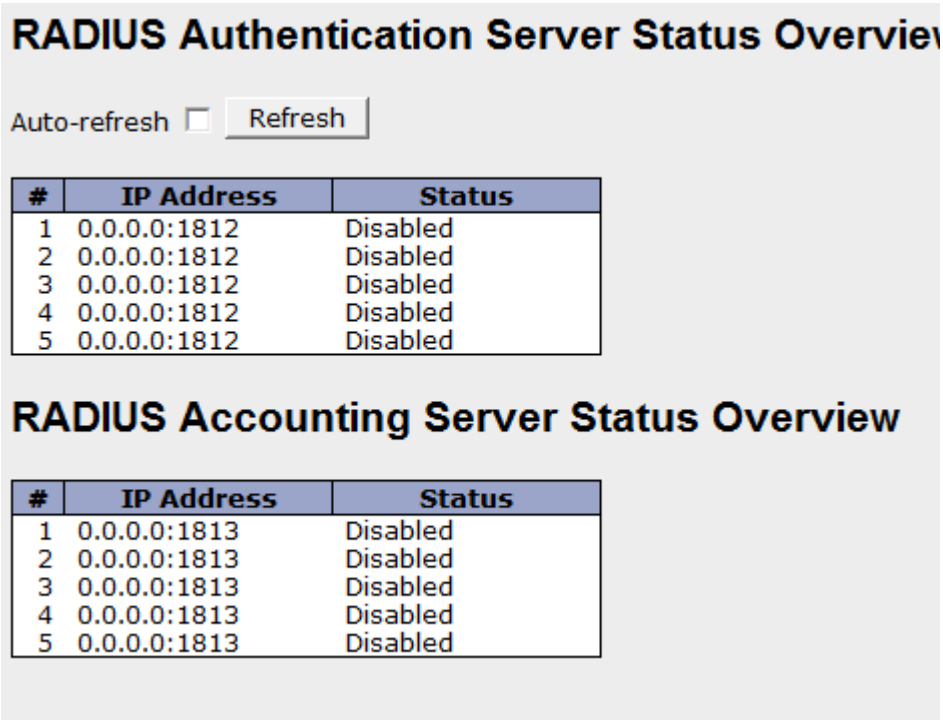
There is one row for each RADIUS Accounting Server.

The following table describes the options available.

Option	Description
Enable	Check to enable the RADIUS Accounting Server
IP Address	IP address of the RADIUS Accounting Server in dotted decimal notation
Port	THE UDP port to use on the RADIUS Accounting Server. If the port is set to 0 (zero) the default port (1813) is used on the RADIUS Authentication Server
Secret	The password (up to 29 characters) shared between the RADIUS Accounting Server and the switch

6.10.2.5 RADIUS Authentication and Accounting Server Status

This page provides an overview of the status of the RADIUS servers configured on the previous pages.



RADIUS Authentication Servers

The following table describes the options available.

Option	Description
IP Address	IP address of the RADIUS Authentication Server in <IP Address><UDP Port>notation
Status	Disabled: The server is disabled Not Ready: The server is enabled but IP communication is not up and running Ready: The server is enabled, IP communication is running and the RADIUS module is ready to accept access attempts Dead (X seconds left): Access attempts were made to the server but it did not reply within the configured timeout. The server has been temporarily disabled but will re-enable when the dead time expires. This state only applies when more than one server is enabled.

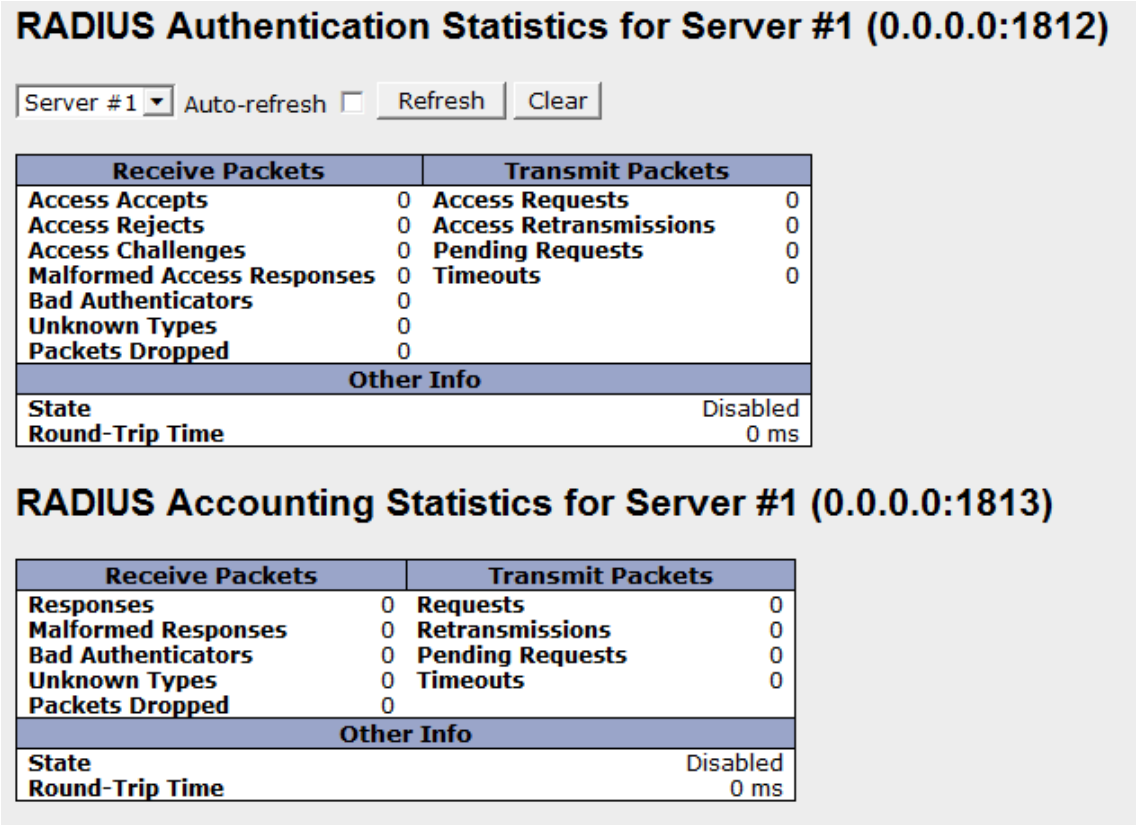
RADIUS Accounting Servers

The following table describes the options available.

Option	Description
IP Address	IP address of the RADIUS Accounting Server in <IP Address><UDP Port>notation
Status	Disabled: The server is disabled Not Ready: The server is enabled but IP communication is not up and running Ready: The server is enabled, IP communication is running and the RADIUS module is ready to accept access attempts Dead (X seconds left): Access attempts were made to the server but it did not reply within the configured timeout. The server has been temporarily disabled but will re-enable when the dead time expires. This state only applies when more than one server is enabled.

6.10.2.6 RADIUS Statistics

This page provides the detailed statistics for a particular RADIUS Server.



Radius Authentication Statistics

Select the appropriate server using the select box. There are seven receive and four transmit counters.

The following table describes the options available.

Option	Description
RECEIVE	
Access Accepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server
Access Rejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server
Access Challenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server
Malformed Access Responses	The number of malformed RADIUS Access-Response packets (valid or invalid) received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.
Bad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.

Unknown Types	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Packets Dropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
TRANSMIT	
Access Requests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
Access Retransmissions	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication servers.
Pending Requests	The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This is incremented when an Access-Request is sent and decremented on receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout or retransmission.
Timeouts	The number of authentication timeouts to the server. After a timeout, the client may retry to the same server (counted as a retransmit as well as a timeout), send to a different server (counted as a Request as well as a timeout) or give up.
OTHER INFO	
State	This shows the state of the server. Disabled: The selected server is disabled Not Ready: The server is enabled but IP communication is not up and running Ready: The server is enabled, IP communications are running and the RADIUS module is ready to accept access attempts. Dead (x seconds left): Access attempts were made to the server but it did not reply within the configured timeout. The server has been temporarily disabled but will re-enable when the dead time expires. This state only applies when more than one server is enabled.
Round-Trip Time	The time interval (ms, granularity 100ms) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. 0ms indicates that ther hasn't been round-trip communications with the server yet

Radius Accounting Statistics

Select the appropriate server using the select box. There are five receive and four transmit counters.

The following table describes the options available.

Option	Description
RECEIVE	
Responses	The number of RADIUS packets (valid or invalid) received from the server
Malformed Responses	The number of malformed RADIUS packets (valid or invalid) received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.
Bad Authenticators	The number of RADIUS packets containing invalid authenticators received from the server.
Unknown Types	The number of RADIUS packets of unknown types that were received from the server on the accounting port.
Packets Dropped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
TRANSMIT	
Requests	The number of RADIUS packets sent to the server. This does not include retransmissions.
Retransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.
Pending Requests	The number of RADIUS packets destined for the server that have not yet timed out or received a response. This is incremented when an Request is sent and decremented on receipt of a Response, timeout or retransmission.
Timeouts	The number of accounting timeouts to the server. After a timeout, the client may retry to the same server (counted as a retransmit as well as a timeout), send to a different server (counted as a Request as well as a timeout) or give up.
OTHER INFO	
State	This shows the state of the server. Disabled: The selected server is disabled Not Ready: The server is enabled but IP communication is not up and running Ready: The server is enabled, IP communications are running and the RADIUS module is ready to accept access attempts. Dead (x seconds left): Access attempts were made to the server but it did not reply within the configured timeout. The server has been temporarily disabled but will re-enable when the dead time expires. This state only applies when more than one server is enabled.
Round-Trip Time	The time interval (ms, granularity 100ms) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. 0ms indicates that ther hasn't been round-trip communications with the server yet

6.11 Warning

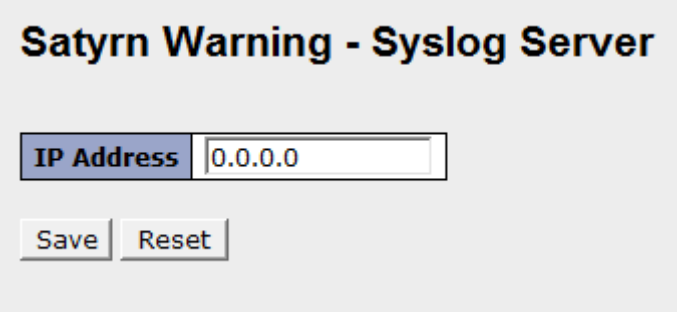
The warning function is very important for managing a switch. You can receive warnings by SYSLOG or SMTP and email. This is used for monitoring the switch status on remote locations. When problems occur, the warning message will be sent to your appointed SYSLOG server or email.

Check the corresponding box to enable the system event warning method you wish to activate. Please note that the checkbox cannot be checked when SYSLOG or SMTP are disabled.

6.11.1 Satyrn Warning

6.11.1.1 Syslog Setting

The Syslog Server can be identified here.

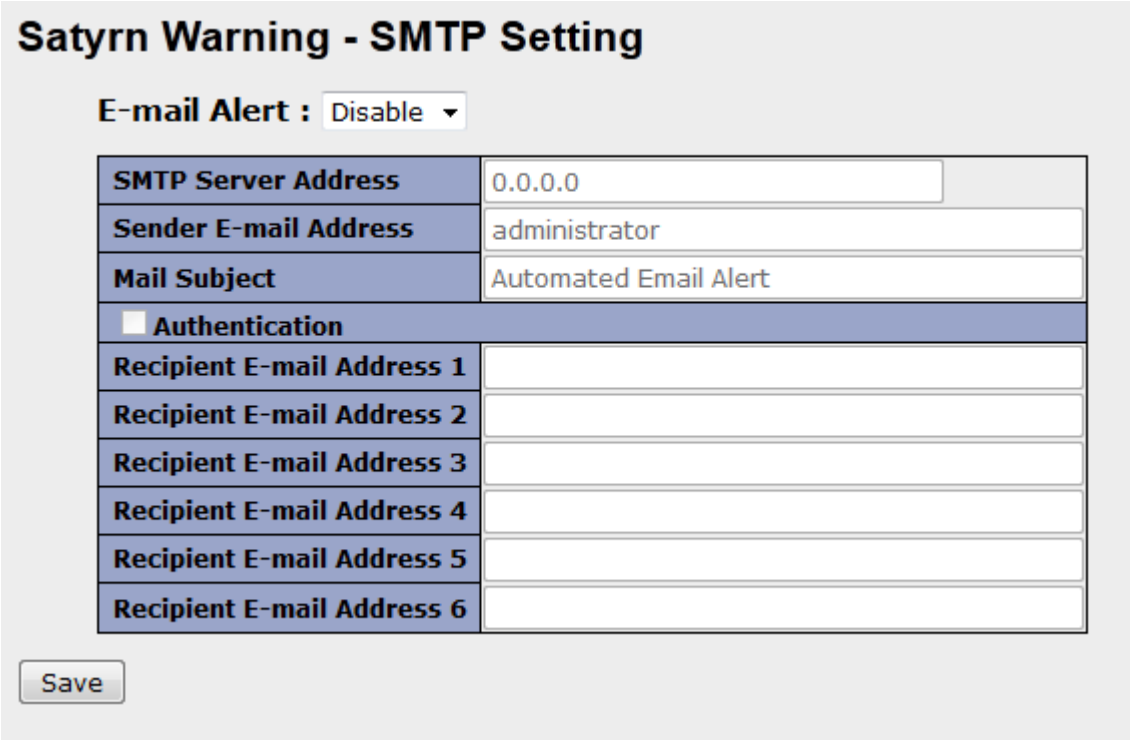


The following table describes the options available.

Option	Description
IP Address	The remote SYSLOG Server IP address.
Apply	Click "**Apply**" to save the configuration.
Help	Show help file.

6.11.1.2 SMTP Settings

Certain events can trigger an e-mail to be sent to a number of recipients informing them of the event. The e-mails can be configured on this page and the events for warning are identified in the next section.

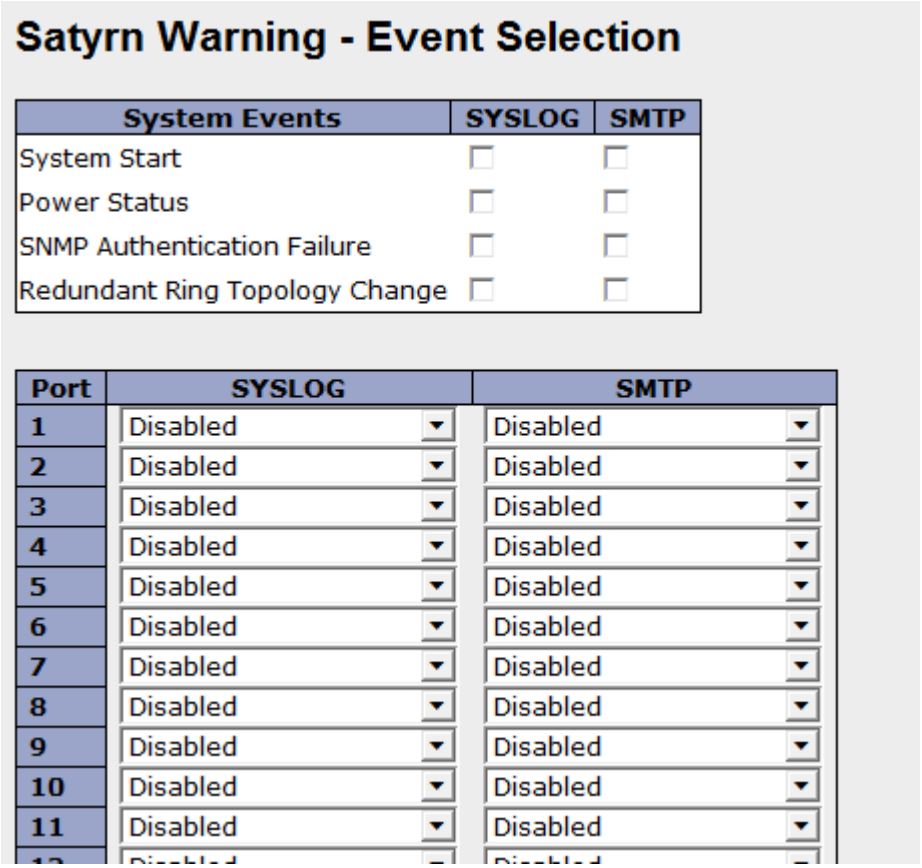


The following table describes the options available.

Option	Description
E-mail alert	Enable/Disable e-mail transmission of events
SMTP Server Address	The SMTP server IP or domain name address
Sender e-mail Address	The e-mail address of the sender
Mail subject	The Subject of the e-mail.
Authentication	Checked if the SMTP server needs authentication.
Recipient e-mail address	E-mail addresses of recipients, up to 6 can be entered

6.11.1.3 Event Selection

The different events that are recorder on the SYSLOG or notified by SMTP are chosen in this section.



The following table describes the options available.

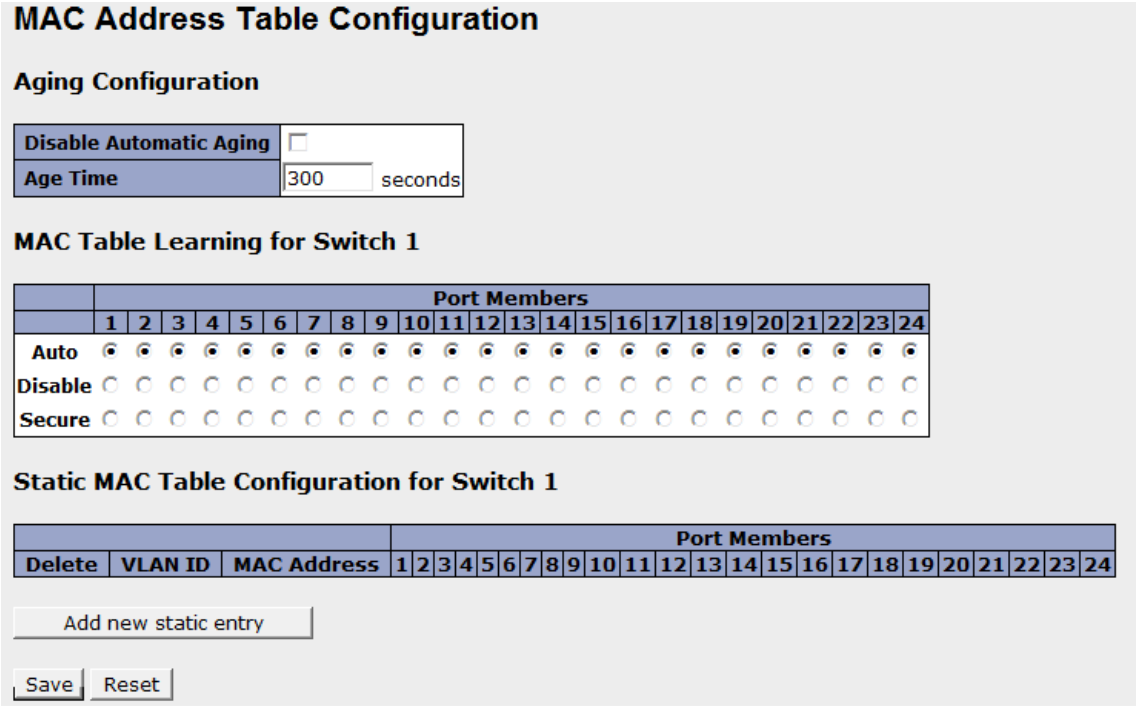
Options	Description
System Start	An alert is generated when the system restarts
Power Status	An alert is generated when power is added or removed
SNMP Authentication Failure	An alert is generated when SNMP Authentication Fails
Redundant Ring Topology Change	An alert is generated when the Redundant Ring Topology is changed
Port Event	An alert is generated when a specific Link is either up or down or when either event occours.

6.12 Monitor and Diagnostics

6.12.1 MAC Table

The MAC Address Table is configured on this page. You can set timeouts for entries in the dynamic MAC Table and configure the static MAC table here.

6.12.1.1 MAC Table Configuration


MAC Address Table Configuration
Aging Configuration
Disable Automatic Aging
Age Time
300
seconds
MAC Table Learning for Switch 1
Port Members
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Auto
Disable
Secure
Static MAC Table Configuration for Switch 1
Delete
VLAN ID
MAC Address
Port Members
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Add new static entry
Save
Reset

Aging Configuration

By default, dynamic entries are removed from the MAC after 300 seconds. This removal is also called aging.

The following table describes the options available.

Option	Description
Aging configuration	Disable Automatic Timing: Check to disable Age Time: Allowed range is 10 to 100,000 secs

MAC Table Learning

If the learning mode for a given port is greyed out, another module (e.g. MAC-Based Authentication under 802.1X) is in control of the mode, so that it cannot be changed by the user.

The following table describes the options available.

Option	Description
MAC Table Learning	Auto: 'Learning' is done automatically as soon as a frame with unknown SMAC is received. Disable: 'Learning' is disabled. Secure: Only static MAC entries are 'learned', all other frames are dropped. **Note:** Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries.

The MAC table is sorted first by VLAN ID and then by MAC address.

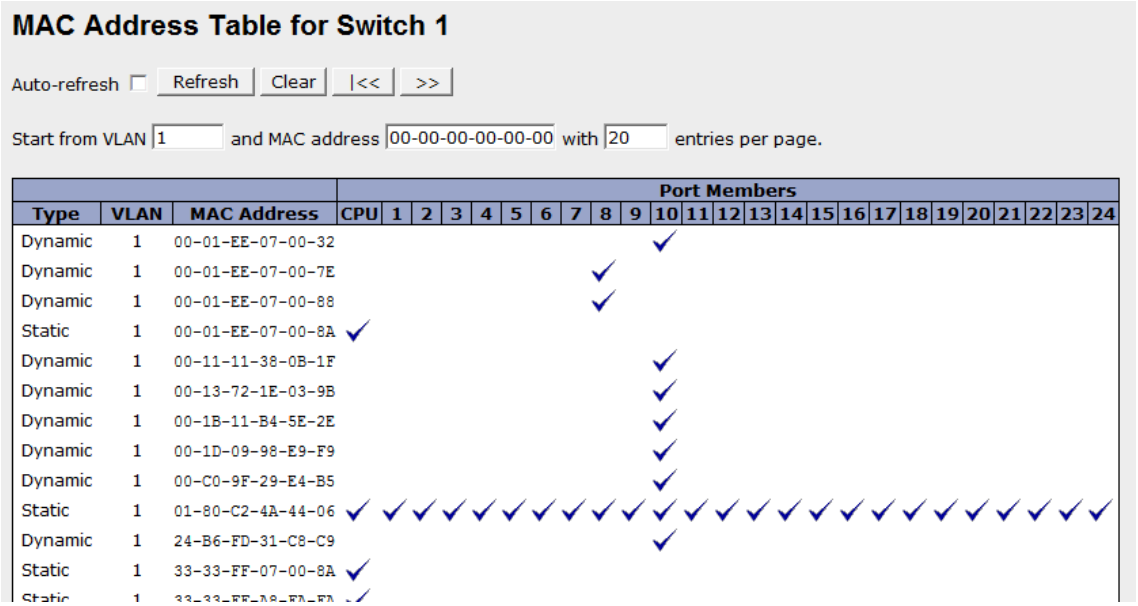
The following table describes the options available.

Option	Description
Delete	Check to delete the entry. It will be removed after the next SAVE.
VLAN ID	The ID of the VLAN for the particular entry
MAC Address	The MAC Address of the particular entry
Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.
Adding a New Static Entry	Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Save".

6.12.1.2 MAC Address Table

Entries in the MAC Table are shown on this page. The MAC Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.

Each page can show up to 999 entries from the MAC table with the default being 20 and will be the first 20 entries from the beginning of the MAC Table starting with the lowest VLAN ID and the lowest MAC address found in the MAC Table.


MAC Address Table for Switch 1
Auto-refresh
Refresh
Clear
|<<
>>
Start from VLAN 1 and MAC address 00-00-00-00-00-00 with 20 entries per page.
Port Members
Type VLAN MAC Address CPU 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Dynamic 1 00-01-EE-07-00-32
Dynamic 1 00-01-EE-07-00-7E
Dynamic 1 00-01-EE-07-00-88
Static 1 00-01-EE-07-00-8A
Dynamic 1 00-11-11-38-0B-1F
Dynamic 1 00-13-72-1E-03-9B
Dynamic 1 00-1B-11-B4-5E-2E
Dynamic 1 00-1D-09-98-E9-F9
Dynamic 1 00-C0-9F-29-E4-B5
Static 1 01-80-C2-4A-44-06
Dynamic 1 24-B6-FD-31-C8-C9
Static 1 33-33-FF-07-00-8A

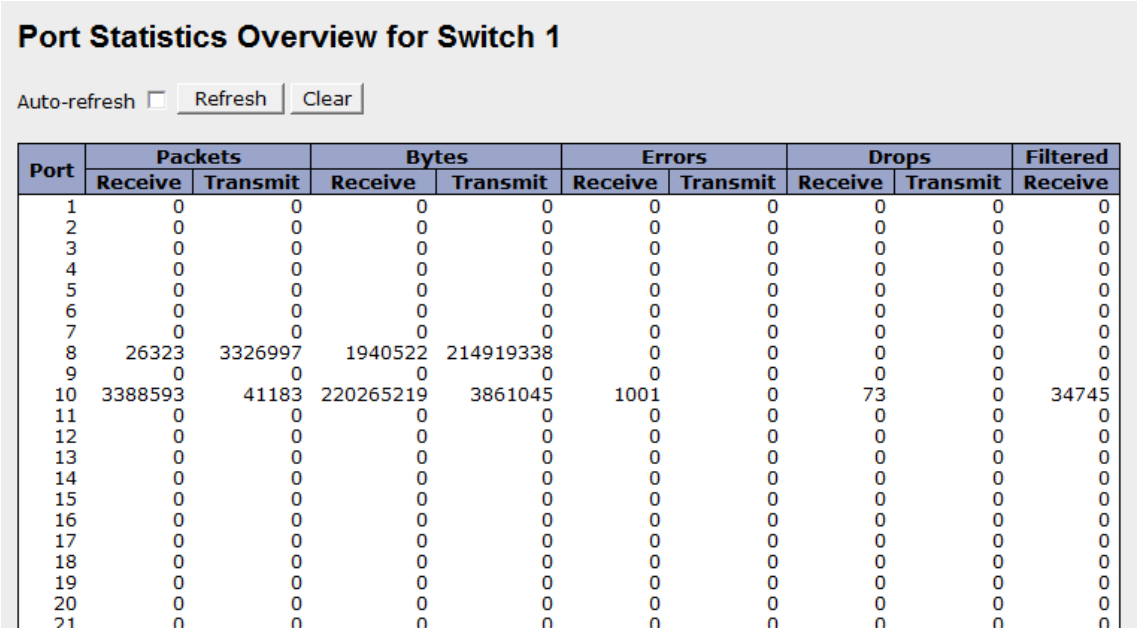
The following table describes the options available.

Option	Description
Type	Indicates whether the entry is a static or dynamic entry.
VLAN	The VLAN ID of the entry
MAC Address	The MAC address of the entry
Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.
Adding a New Static Entry	Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Save".
Auto Refresh	Automatically refreshes the page at regular intervals.
Refresh	Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.
Clear	Flushes all dynamic entries.
|<<	Updates the table starting from the first entry in the MAC Table, i.e. the entry with the lowest VLAN ID and MAC address.
>>	Updates the table, starting with the entry after the last entry currently displayed.
Start from VLAN and MAC address	Selects the starting point of the table
Entries per page	Identifies the size of the displayed table

6.12.2 Port Statistics

6.12.2.1 Port Traffic Overview

This page provides an overview of general traffic statistics for all switch ports.



Port Statistics Overview for Switch 1

Auto-refresh ☐ Refresh Clear

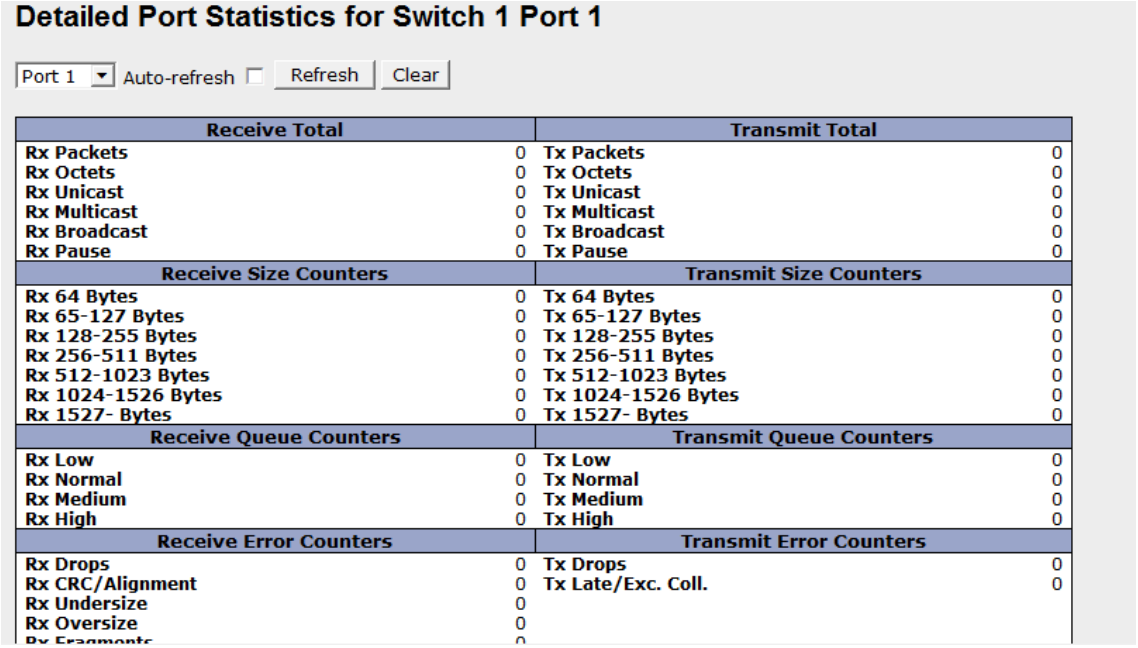
Port	Packets		Bytes		Errors		Drops		Filtered
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	26323	3326997	1940522	214919338	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	3388593	41183	220265219	3861045	1001	0	73	0	34745
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0

The following table describes the options available.

Option	Description
Port	The logical port for the settings contained in the same row.
Packets	The number of received and transmitted packets per port.
Bytes	The number of received and transmitted bytes per port.
Errors	The number of frames received in error and the number of incomplete transmissions per port.
Drops	The number of frames discarded due to ingress or egress congestion.
Filtered	The number of received frames filtered by the forwarding process.

6.12.2.2 Detail Port Statistics

This page provides detailed traffic statistics for a specific switch port. Use the port select box to display details for a specific switch port.



The following table describes the options available.

Option	Description
Receive and Transmit Total	
Rx & Tx Packets	The number of received and transmitted (good and bad) packets.
Rx & Tx Octets	The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.
Rx & Tx Unicast	The number of received and transmitted (good and bad) unicast packets.
Rx & Tx Multicast	The number of received and transmitted (good and bad) multicast packets.
Rx & Tx Broadcast	The number of received and transmitted (good and bad) broadcast packets.
Rx & Tx Pause	A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.
Receive and Transmit Size Counters	The number of received and transmitted (good and bad) packets split into frame sizes.
Receive and Transmit Queue Counters	The number of received and transmitted packets per input and output queue.
Receive Error Counters	
Rx Drops	The number of frames dropped due to lack of receive buffers or egress congestion.
Rx CRC/Alignment	The number of frames received with CRC or alignment errors.
Rx Undersize	The number of short (less than 64 bytes) frames received with valid CRC.

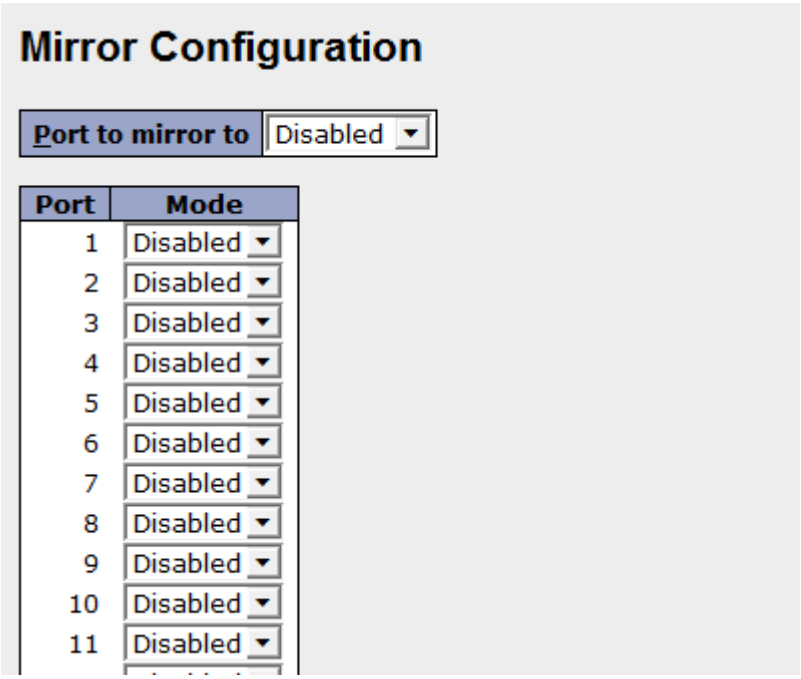
Rx Oversize	The number of long (longer than the configured maximum frame length for this port) frames received with valid CRC.
Rx Fragments	The number of (less than 64 bytes) frames received with invalid CRC.
Rx Jabber	The number of long (longer than the configured maximum frame length for this port) frames received with invalid CRC.
Rx Filtered	The number of received frames filtered by the forwarding process.
Transmit Error Counters	
Tx Drops	The number of frames dropped due to output buffer congestion.
Tx Late/Exc. Coll.	The number of frames dropped due to excessive or late collisions.

6.12.3 Port Monitoring (Mirroring)

Port Mirroring is configured on this page.

To debug network problems, selected traffic can be copied, or mirrored, to a mirror port where a frame analyser can be attached to analyse the frame flow. The traffic to be copied to the mirror port is selected as follows:

- All frames received on a given port (also known as ingress or source mirroring).
- All frames transmitted on a given port (also known as egress or destination mirroring).

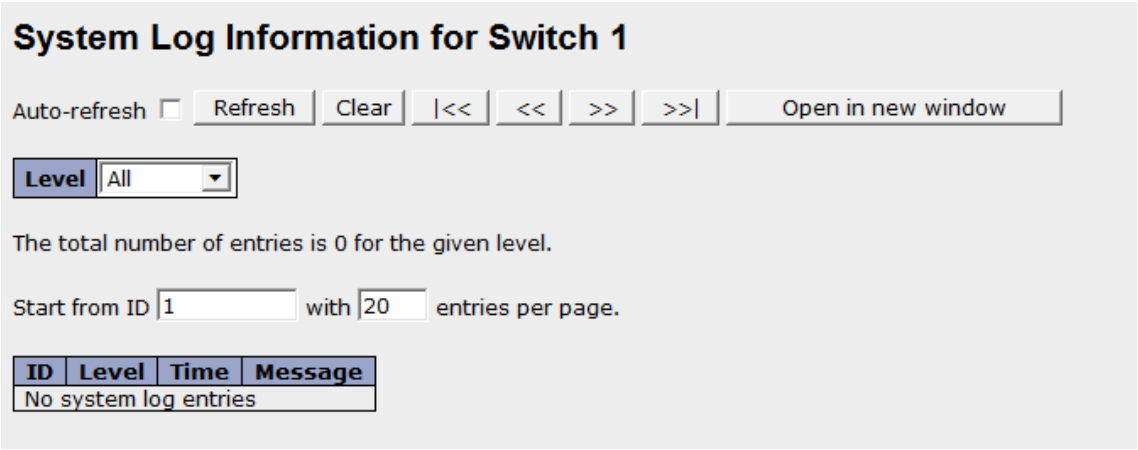


The following table describes the options available.

Option	Description
Port to Mirror to	Frames from ports that have either source (Rx) or destination (Tx) mirroring enabled are mirrored to this port.
Port	The logical port for the settings contained in the same row
Mode	Rx only: Frames received at this port are mirrored to the mirror port. Frames transmitted are not mirrored. Tx only: Frames transmitted from this port are mirrored to the mirror port. Frames received are not mirrored. Disabled: Neither frames transmitted nor frames received are mirrored. Enabled: Frames received and frames transmitted are mirrored to the mirror port. Note: For a given port, a frame is only transmitted once. It is therefore not possible to mirror Tx frames for the mirror port. Because of this, mode for the selected mirror port is limited to Disabled or Rx only.

6.12.4 System Log

The switch system log information is provided here.



The following table describes the options available.

Option	Description
Auto-refresh	Automatic refresh of the page at regular intervals
Refresh	: Updates the system log entries, starting from the current entry ID
Clear	Flushes all system log entries.
|<<	Updates the system log entries, starting from the first available entry ID.

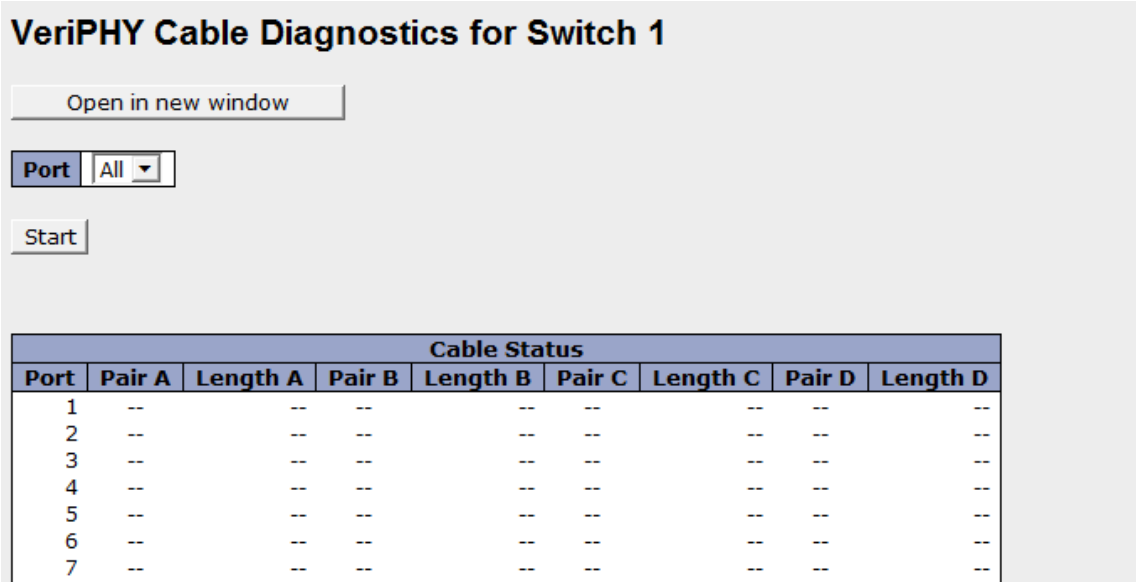
<<	: Updates the system log entries, ending at the last entry currently displayed.
>>	: Updates the system log entries, starting from the last entry currently displayed.
>>|	: Updates the system log entries, ending at the last available entry ID.
ID	The ID of the System Log entry
Level	The level of the system log entry. The following level types are supported. Info: Information level of the system log. Warning: Warning level of the system log. Error: Error level of the system log. All: All levels.
Time	The time of the system log entry.
Message	The message of the system log entry.

6.12.5 Cable Diagnostics

This page is used for running the VeriPHY Cable Diagnostics.

Click Start to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table.

Note that VeriPHY is only accurate for cables of length 7 - 140 metres. 10 and 100 Mbps ports will be linked down while running VeriPHY so running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.


VeriPHY Cable Diagnostics for Switch 1
Open in new window
Port
All
Start
Cable Status
Port Pair A Length A Pair B Length B Pair C Length C Pair D Length D
1 -- -- -- -- -- -- -- -- --
2 -- -- -- -- -- -- -- -- --
3 -- -- -- -- -- -- -- -- --
4 -- -- -- -- -- -- -- -- --
5 -- -- -- -- -- -- -- -- --
6 -- -- -- -- -- -- -- -- --
7 -- -- -- -- -- -- -- -- --

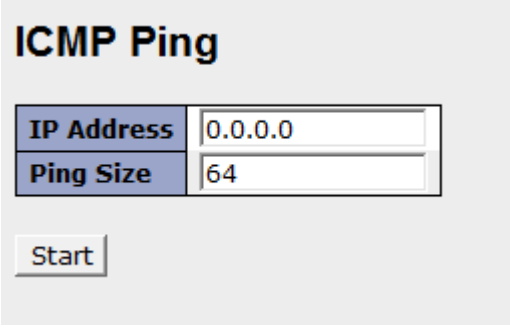
The following table describes the options available.

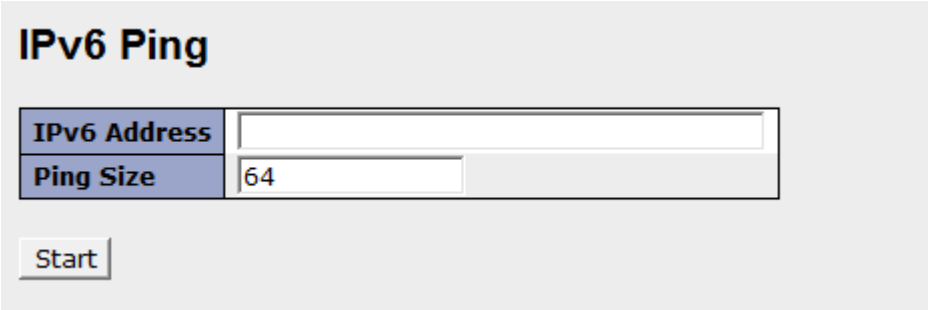
Option	Description
Port	The port where you are requesting VeriPHY Cable Diagnostics.
Cable Status	Port: Port number. Pair: The status of the cable pair. Length: The length (in meters) of the cable pair.

6.12.6 ICMP & ICMPv6 Ping

This page allows you to issue ICMP Ping packets to troubleshoot IP connectivity issues.

Clicking Start transmits 5 ICMP are transmitted and the sequence number and roundtrip time are displayed for reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.





The following table describes the options available.

Option	Description
IP/IPv6 Address	The destination IP Address.
Ping Size	The payload size of the ICMP packet. Values range from 8 bytes to 1400 bytes.

6.13 Power over Ethernet

Power Over Ethernet is used to transmit electrical power, to remote devices over standard Ethernet cable. It could for example be used for powering IP telephones, wireless LAN access points and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.

6.13.1 PoE Configuration

This page allows the user to inspect and configure the current PoE port settings.

There are three modes for configuring how the ports/Powered Device (PD) reserve power.

Allocated mode: The user allocates the amount of power that each port may reserve with the allocated/reserved power specified in the Maximum Power fields.

Class mode: Each port automatically determines how much power to reserve according to the class the connected PD belongs to. There are 3 classes 4, 7 and 15.4 Watts. In this mode the Maximum Power fields have no effect.

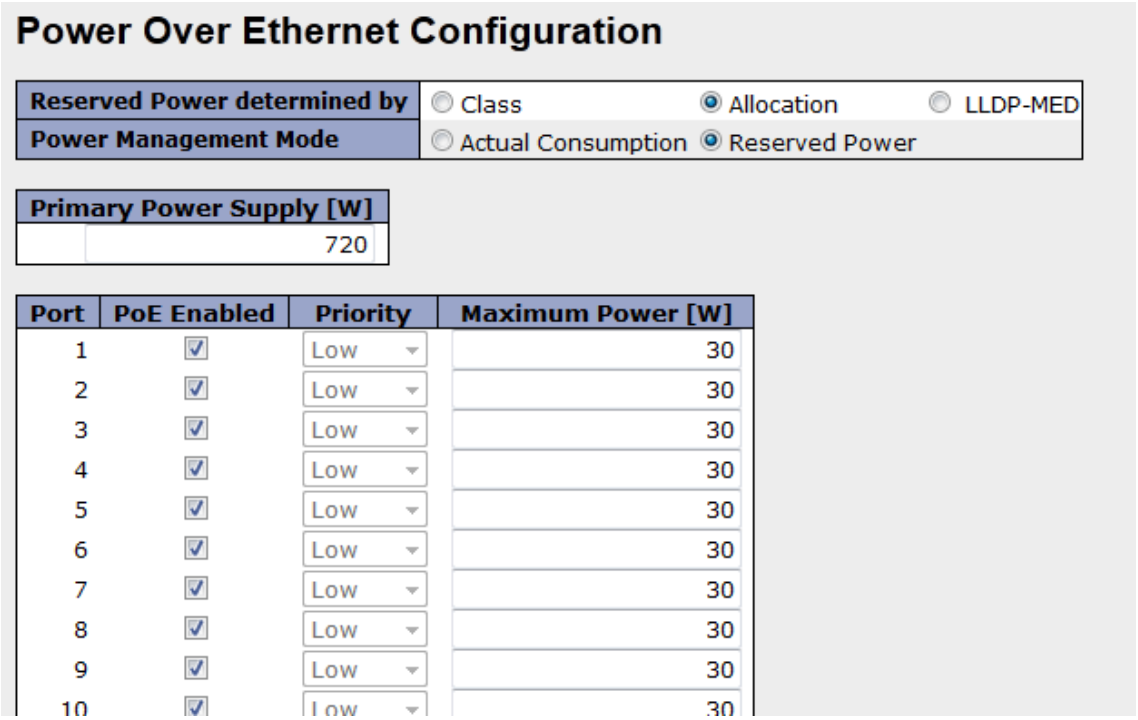
LLDP-MED mode: Each port determines the amount power it reserves by exchanging PoE information using the LLDP protocol. If no LLDP information is available for a port, the port will reserve power using the class mode. In this mode the Maximum Power fields have no effect

In all modes, if a port uses more power than the reserved power for the port, the port is shut down.

There are 2 modes for configuring when to the ports are shut down.

Actual Consumption: The ports are shut down when the actual power consumption for all ports exceeds the amount of power available from the power supply or if the power consumption for a given port exceeds the reserved power for that port. The ports are shut down according to the port's priority. If two ports have the same priority the port with the highest port number is shut down.

Reserved Power: In this mode the ports are shut down when total reserved power exceeds the amount of power that the power supply can deliver. In this mode the port power is not turned on if the PD requests more power than is available.

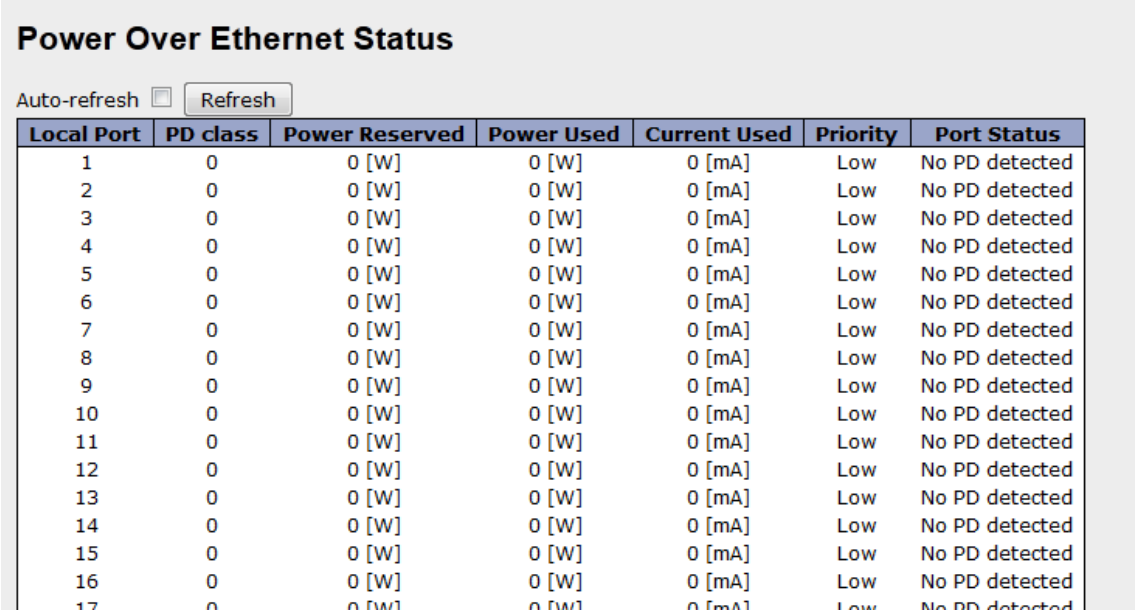


The following table describes the options available.

Option	Description
Port	The logical port
PoE enabled	If checked enables power to be delivered to the port
Priority	Port priority used to control the shutdown of power to the port. There are three levels of power priority Low, High and Critical.
Maximum Power	The maximum power in watts that can be delivered to The PD. The maximum allowed value is 102.3 W.

6.13.2 PoE Status

This page allows the user to inspect the current status for all PoE ports.



Power Over Ethernet Status

Auto-refresh ☐ Refresh

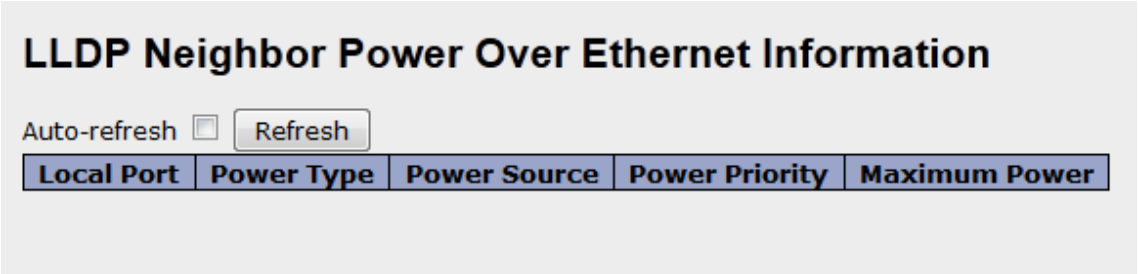
Local Port	PD class	Power Reserved	Power Used	Current Used	Priority	Port Status
1	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
2	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
3	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
4	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
5	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
6	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
7	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
8	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
9	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
10	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
11	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
12	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
13	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
14	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
15	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
16	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected
17	0	0 [W]	0 [W]	0 [mA]	Low	No PD detected

The following table describes the options available.

Option	Description
Local Port	The logical port
Power Reserved	The power the PD has reserved.
Power used	The power the PD is using.
Priority	The configured priority for the port.
Port Status	The port's status

6.13.3 LLDP Neighbour Information

This page provides a status overview for all LLDP PoE neighbours.

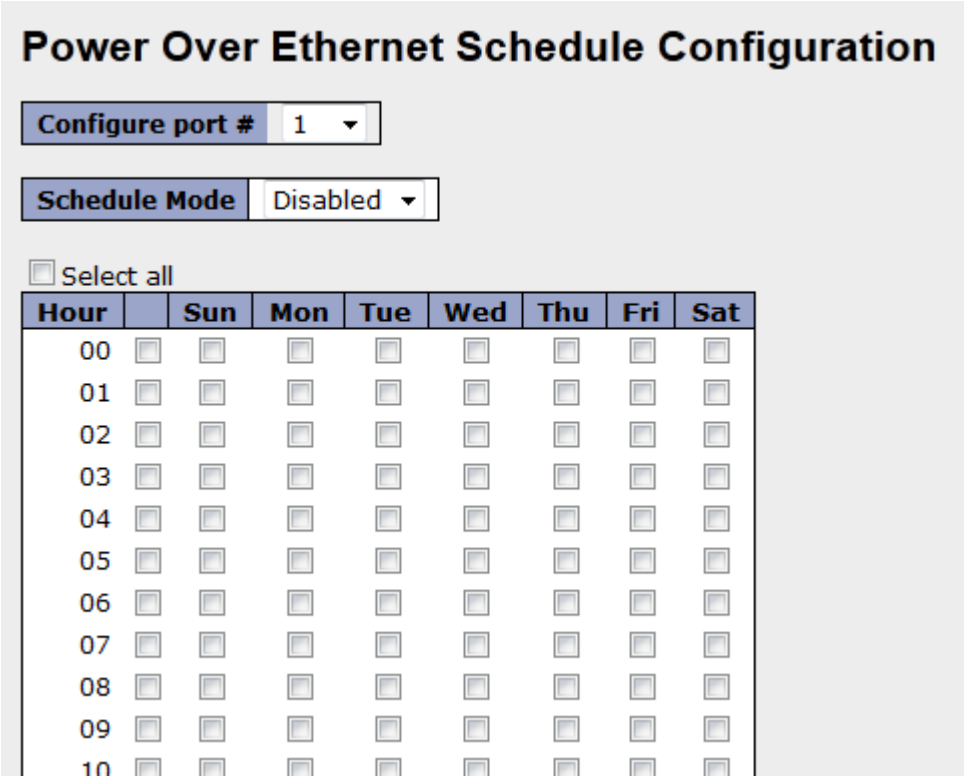


The following table describes the options available.

Option	Description
Local Port	The logical port
Type	PSE – Power Sourcing Entity PD – Powered Device Reserved – Unknown type
Source	The power source being used by the PSE or PD. If PSE, it can either run on its Primary Power Source or its Backup Power Source. If it is not known which is being used it is indicated as "Unknown" If PD, it can either run on its local power supply or use the PSE as power source. It can also use both its local power supply and the PSE. If it is not known what power supply the PD is using it is indicated as "Unknown".
Priority	The configured priority for the PD or PSE.
Power Value	The maximum power required by a PD from a PSE, or the minimum power a PSE can source over a maximum length cable based on its current configuration. The maximum allowed value is 102.3 W. If the device indicates value higher than 102.3 W, it is represented as "reserved"

6.13.4 PoE Schedule

Use this page to schedule the times that power is sent to the PD.

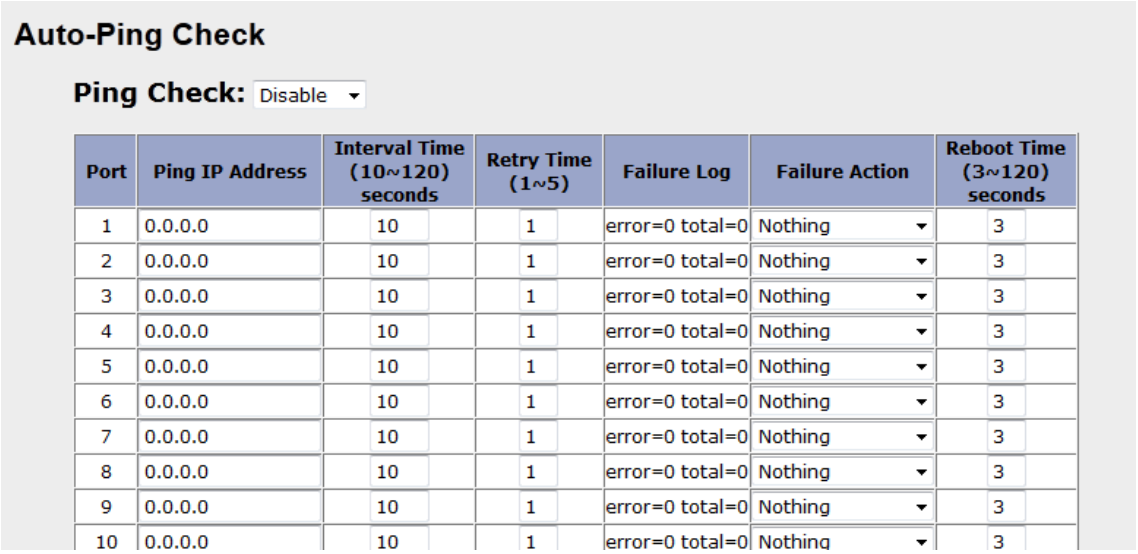


The following table describes the options available.

Option	Description
Configure port #	The port to be configured
Schedule mode	Enable/Disable the PoE Schedule.
Hour	The hours in the day the Schedule applies power to the port.
Day	The days of the week the Schedule applies power to the port.

6.13.5 Auto Ping Check

To check the health of the PD connected to the ports on the switch an automatic ping is sent to the PD. This section allows you to configure that process and carry out appropriate actions to restore the PD if it needs it.

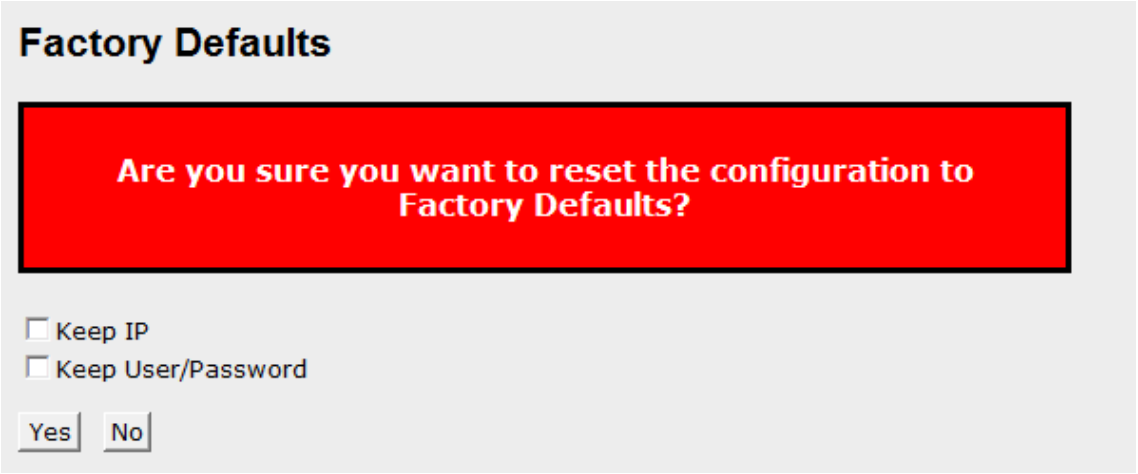

Auto-Ping Check
Ping Check: Disable
Port
Ping IP Address
Interval Time (10~120) seconds
Retry Time (1~5)
Failure Log
Failure Action
Reboot Time (3~120) seconds
1 0.0.0.0 10 1 error=0 total=0 Nothing 3
2 0.0.0.0 10 1 error=0 total=0 Nothing 3
3 0.0.0.0 10 1 error=0 total=0 Nothing 3
4 0.0.0.0 10 1 error=0 total=0 Nothing 3
5 0.0.0.0 10 1 error=0 total=0 Nothing 3
6 0.0.0.0 10 1 error=0 total=0 Nothing 3
7 0.0.0.0 10 1 error=0 total=0 Nothing 3
8 0.0.0.0 10 1 error=0 total=0 Nothing 3
9 0.0.0.0 10 1 error=0 total=0 Nothing 3
10 0.0.0.0 10 1 error=0 total=0 Nothing 3

The following table describes the options available.

Option	Description
Ping Check	Enable/Disable Auto Ping
Port	The logical port to be Auto Pinged
Ping IP address	The IP Address of target.
Interval Time	The time between Pings (10 to 120 seconds)
Retry Time	Ping retry times (1 to 5)
Failure Log	Record of the failures
Failure Action	Nothing : Do nothing. Restart Forever : Always restart the PoE when failure occurs Restart Once : Only once restart the PoE when failure occurs Power On : Turn on the PoE when failure happen. Power Down : Turn off the PoE when failure happen
Reboot Time	The time intervals (3 to 120 seconds) between reboots when the Failure Action is set as Restart Forever.

6.14 Factory Defaults

You can reset the configuration of the stack switch on this page. The IP configuration will be retained.

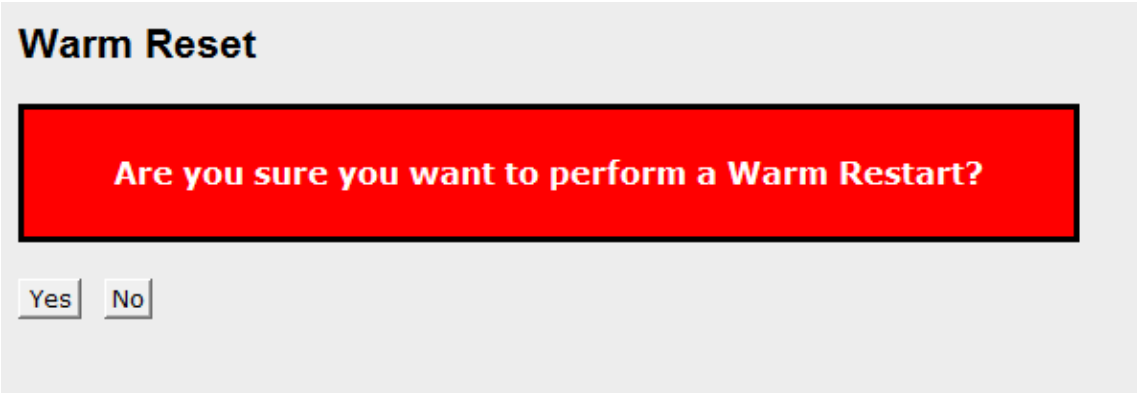


The following table describes the options available.

Option	Description
Keep IP	Check to maintain the IP address after reset
Keep User/Password	Check to maintain the User Password after reset
YES	Click to reset the configuration to the Factory Default settings.
NO	Click to return to the Port State page without resetting the configuration

6.15 System Reboot

You can reset the switch on this page. After a reset, the system will boot normally as if you had turned on the device.



The following table describes the options available.

Option	Description
YES	Click to reboot device.
NO	Click to return to the Port State page without rebooting.

7 Command Line Interface Management

7.1 About CLI Management

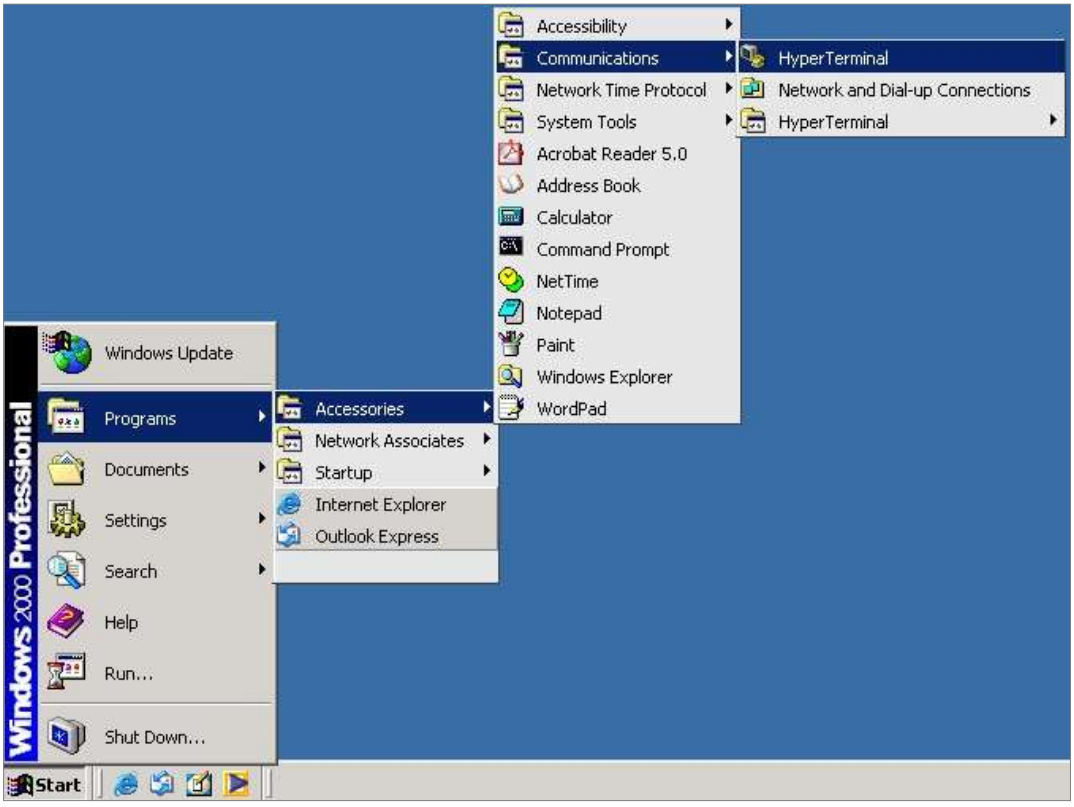
Besides WEB-base management, IES-3073GC also support CLI management. You can use console or telnet to manage the switch by CLI.

7.1.1 CLI Management by RS-232 Serial Console (115200, 8, none, 1, none)

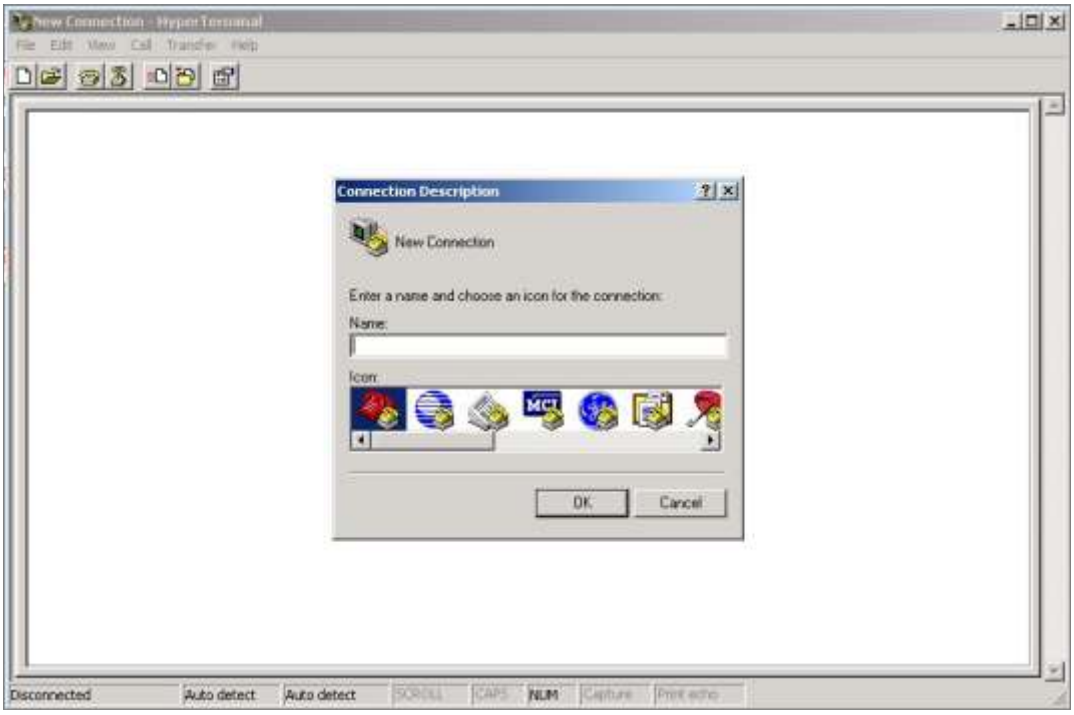
Before Configuring by RS-232 serial console, use an RJ45 to DB9-F cable to connect the switch's RS-232 Console port to your PC's COM port.

Follow the steps below to access the console via RS-232 serial cable.

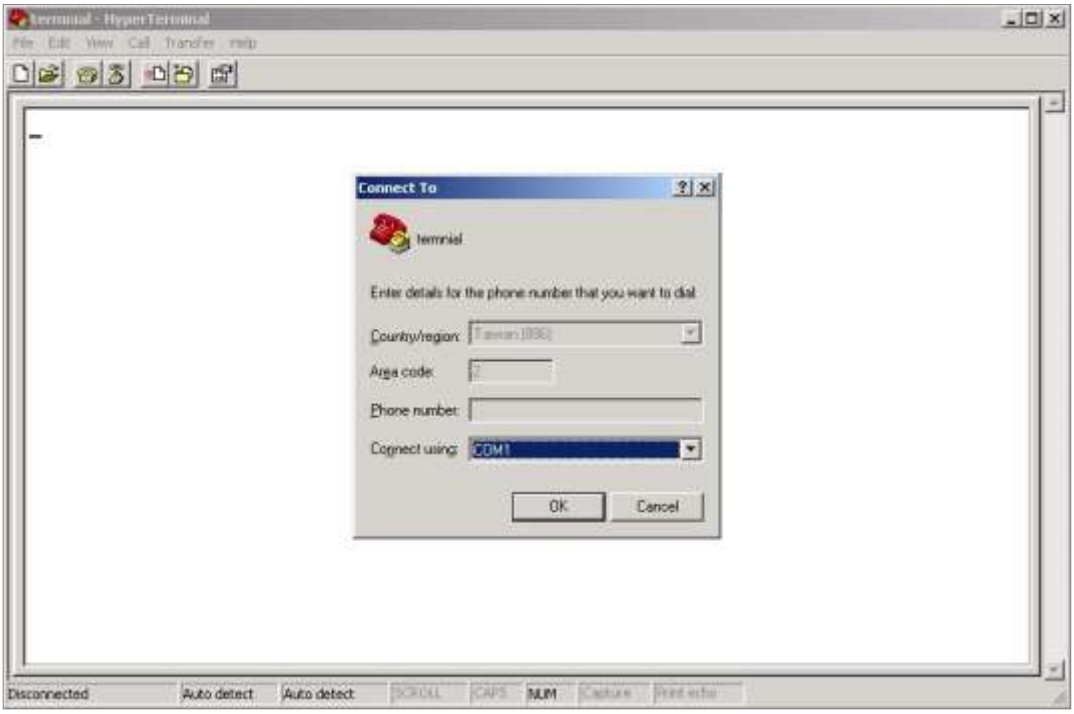
Step 1. From the Windows desktop, click on Start -> Programs -> Accessories -> Communications -> Hyper Terminal



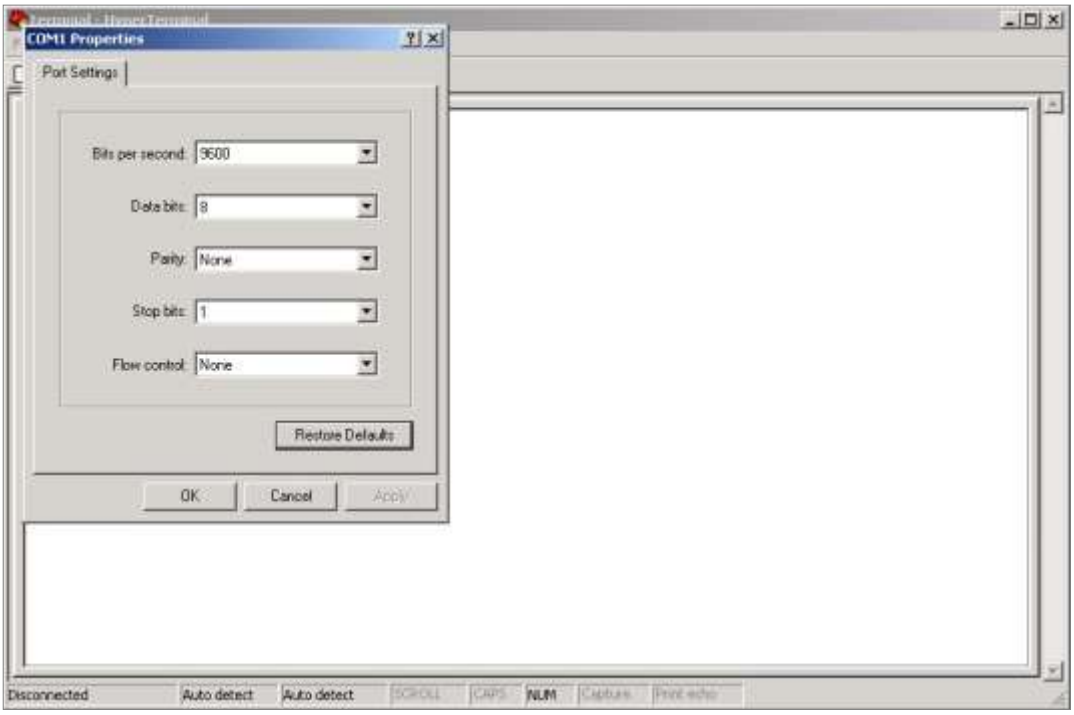
Step 2. Enter a name for the new connection.



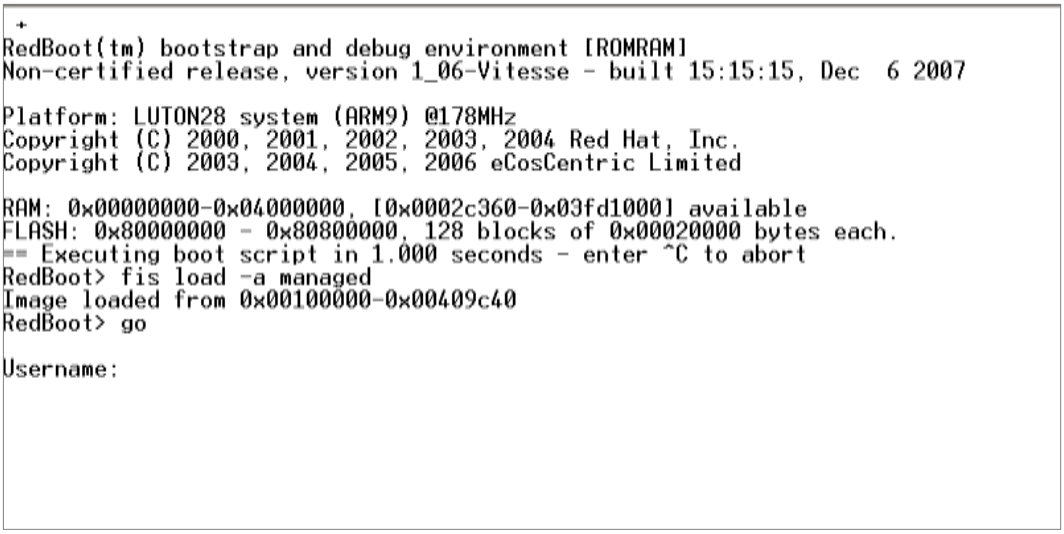
Step 3. Select a COM port number.



Step 4. Set the COM port properties to: 115200 for Bits per second, 8 for Data bits, None for Parity, 1 for Stop bits and none for Flow control.



Step 5. The Console login screen will appear. Enter the Username and Password, then press "**Enter**".


RedBoot(tm) bootstrap and debug environment [ROMRAM]
Non-certified release, version 1_06-Vitesse - built 15:15:15, Dec 6 2007
Platform: LUTON28 system (ARM9) @178MHz
Copyright (C) 2000, 2001, 2002, 2003, 2004 Red Hat, Inc.
Copyright (C) 2003, 2004, 2005, 2006 eCosCentric Limited
RAM: 0x00000000-0x04000000, [0x0002c360-0x03fd1000] available
FLASH: 0x80000000 - 0x80800000, 128 blocks of 0x00020000 bytes each.
== Executing boot script in 1.000 seconds - enter ^C to abort
RedBoot> fis load -a managed
Image loaded from 0x00100000-0x00409c40
RedBoot> go
Username:

7.1.2 CLI Management by Telnet

Users can use "**TELNET**" to configure the switches. The default values are:

IP Address: **192.168.10.1**

Subnet Mask: **255.255.255.0**

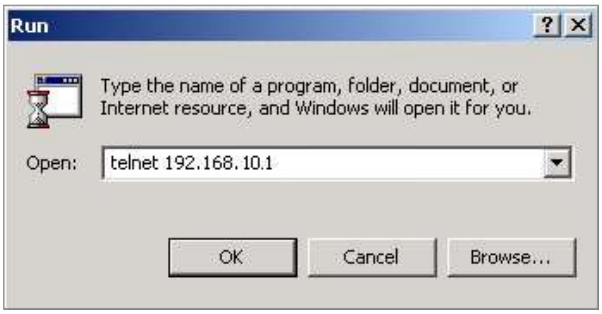
Default Gateway: **192.168.10.254**

User Name: **root**

Password: **root**

Follow the steps below to access the console via Telnet.

Step 1. Telnet to the IP address of the switch from the Windows "**Run**" command or from the MS-DOS prompt as below.



Step 2. The Login screen will appear. Enter the Username and Password, then press "**Enter**"

7.2 Satyrn Groups

```
Command Groups:
---------------
System     : System settings and reset options
Syslog     : Syslog Server Configuration
IP         : IP configuration and Ping
Auth       : Authentication
Port       : Port management
Aggr       : Link Aggregation
LACP       : Link Aggregation Control Protocol
STP        : Spanning Tree Protocol
Dot1x      : IEEE 802.1X port authentication
IGMP       : Internet Group Management Protocol snooping
LLDP       : Link Layer Discovery Protocol
MAC        : MAC address table
VLAN       : Virtual LAN
PVLAN      : Private VLAN
QoS        : Quality of Service
ACL        : Access Control List
Mirror     : Port mirroring
Config     : Load/Save of configuration via TFTP
SNMP       : Simple Network Management Protocol
Firmware   : Download of firmware via TFTP
Fault      : Fault Alarm Configuration
```

7.2.1 System

System>	Configuration [all] [<port_list>]
	Reboot
	Restore Default [keep_ip]
	Contact [<contact>]
	Name [<name>]
	Location [<location>]
	Description [<description>]
	Password <password>
	Username [<username>]
	Timezone [<offset>]
	Log [<log_id>] [all|info|warning|error] [clear]

7.2.2 Syslog

Syslog>	ServerConfiguration [<ip_addr>]

7.2.3 IP

IP>	Configuration
	DHCP [enable|disable]
	Setup [<ip_addr>] [<ip_mask>] [<ip_router>] [<vid>]
	Ping <ip_addr_string> [<ping_length>]
	SNTP [<ip_addr_string>]

7.2.4 Auth

Auth>	Configuration
	Timeout [<timeout>]
	Deadtime [<dead_time>]
	RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]
	ACCT_RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]
	Client [console|telnet|ssh|web] [none|local|radius] [enable|disable]
	Statistics [<server_index>]

7.2.5 Port

Port>	Configuration [<port_list>]
	State [<port_list>] [enable|disable]
	Mode [<port_list>] [10hdx|10fdx|100hdx|100fdx|1000fdx|auto]
	Flow Control [<port_list>] [enable|disable]
	MaxFrame [<port_list>] [<max_frame>]
	Power [<port_list>] [enable|disable|actiphy|dynamic]
	Excessive [<port_list>] [discard|restart]
	Statistics [<port_list>] [<command>]
	VeriPHY [<port_list>]

7.2.6 Aggr

Aggr>	Configuration
	Add <port_list> [<aggr_id>]
	Delete <aggr_id>
	Lookup [<aggr_id>]
	Mode [smac|dmac|ip|port] [enable|disable]

7.2.7 LACP

LACP>	Configuration [<port_list>]
	Mode [<port_list>] [enable|disable]
	Key [<port_list>] [<key>]
	Role [<port_list>] [active|passive]
	Status [<port_list>]
	Statistics [<port_list>] [clear]

7.2.8 STP

STP>	Configuration
	Version [<stp_version>] Non-certified release, v
	Txhold [<holdcount>]lt 15:15:15, Dec 6 2007
	MaxAge [<max_age>]
	FwdDelay [<delay>]
	bpduFilter [enable|disable]
	bpduGuard [enable|disable]
	recovery [<timeout>]
	CName [<config-name>] [<integer>]
	Status [<msti>] [<port_list>]
	Msti Priority [<msti>] [<priority>]

	Msti Map [<msti>] [clear]
	Msti Add <msti> <vid>
	Port Configuration [<port_list>]
	Port Mode [<port_list>] [enable|disable]
	Port Edge [<port_list>] [enable|disable]
	Port AutoEdge [<port_list>] [enable|disable]
	Port P2P [<port_list>] [enable|disable|auto]
	Port RestrictedRole [<port_list>] [enable|disable]
	Port RestrictedTcn [<port_list>] [enable|disable]
	Port bpduGuard [<port_list>] [enable|disable]
	Port Statistics [<port_list>]
	Port Mcheck [<port_list>]
	Msti Port Configuration [<msti>] [<port_list>]
	Msti Port Cost [<msti>] [<port_list>] [<path_cost>]
	Msti Port Priority [<msti>] [<port_list>] [<priority>]

7.2.9 Dot1x

Dot1x>	Configuration [<port_list>]
	Mode [enable|disable]
	State [<port_list>] [macbased|auto|authorized|unauthorized]
	Authenticate [<port_list>] [now]
	Reauthentication [enable|disable]
	Period [<reauth_period>]
	Timeout [<eapol_timeout>]
	Statistics [<port_list>] [clear|eapol|radius]
	Clients [<port_list>] [all|<client_cnt>]
	Agetime [<age_time>]
	Holdtime [<hold_time>]

7.2.10 IGMP

IGMP>	Configuration [<port_list>]
	Mode [enable|disable]
	State [<vid>] [enable|disable]
	Querier [<vid>] [enable|disable]
	Fastleave [<port_list>] [enable|disable]
	Router [<port_list>] [enable|disable]
	Flooding [enable|disable]
	Groups [<vid>]
	Status [<vid>]

7.2.11 LLDP

LLDP>	Configuration [<port_list>]
	Mode [<port_list>] [enable|disable|rx|tx]
	Optional_TLV [<port_list>][port_descr|sys_name|sys_descr|sys_capa|mgmt_addr] [enable|disable]
	Interval [<interval>]
	Hold [<hold>]
	Delay [<delay>]
	Reinit [<reinit>]
	Info [<port_list>]
	Statistics [<port_list>] [clear]

7.2.12 MAC

MAC>	Configuration [<port_list>]
	Add <mac_addr> <port_list> [<vid>]
	Delete <mac_addr> [<vid>]
	Lookup <mac_addr> [<vid>]

	Agetime [<age_time>]
	Learning [<port_list>] [auto|disable|secure]
	Dump [<mac_max>] [<mac_addr>] [<vid>]
	Statistics [<port_list>]
	Flush

7.2.13 VLAN

VLAN>	Configuration [<port_list>]
	Aware [<port_list>] [enable|disable]
	PVID [<port_list>] [<vid>|none]
	FrameType [<port_list>] [all|tagged]
	Add <vid> [<port_list>]
	Delete <vid>
	Lookup [<vid>]

7.2.14 PVLAN

PVLAN>	Configuration [<port_list>]
	Add <pvlan_id> [<port_list>]
	Delete <pvlan_id>
	Lookup [<pvlan_id>]
	Isolate [<port_list>] [enable|disable]

7.2.15 QOS

QoS>	Configuration [<port_list>]
	Classes [<class>]
	Default [<port_list>] [<class>]
	Tagprio [<port_list>] [<tag_prio>]

	QCL Port [<port_list>] [<qcl_id>]
	QCL Add [<qcl_id>] [<qce_id>] [<qce_id_next>] (etype <etype>) | (vid <vid>) | (port <udp_tcp_port>) | (dscp <dscp>) | (tos <tos_list>) | (tag_prio <tag_prio_list>) <class>
	QCL Delete <qcl_id> <qce_id>
	QCL Lookup [<qcl_id>] [<qce_id>]
	Mode [<port_list>] [strict|weighted]
	Weight [<port_list>] [<class>] [<weight>]
	Rate Limiter [<port_list>] [enable|disable] [<bit_rate>]
	Shaper [<port_list>] [enable|disable] [<bit_rate>]
	Storm Unicast [enable|disable] [<packet_rate>]
	Storm Multicast [enable|disable] [<packet_rate>]
	Storm Broadcast [enable|disable] [<packet_rate>]

7.2.16 ACL

ACL>	Configuration [<port_list>]
	Action [<port_list>] [permit|deny] [<rate_limiter>] [<port_copy>] [<logging>] [<shutdown>] Policy [<port_list>] [<policy>]
	Rate [<rate_limiter_list>] [<packet_rate>]

	Add [<ace_id>] [<ace_id_next>] [switch | (port <port>) | (policy <policy>)] [<vid>] [<tag_prio>] [<dmac_type>] [(etype [<etype>] [<smac>] [<dmac>]) | (arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>]) | (ip [<sip>] [<dip>] [<protocol>] [<ip_flags>]) | (icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>]) | (udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>]) | (tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>])] [permit|deny] [<rate_limiter>] [<port_copy>] [<logging>] [<shutdown>] Delete <ace_id>
	Lookup [<ace_id>]
	Clear

7.2.17 Mirror

Mirror>	Configuration [<port_list>]
	Port [<port>|disable]
	Mode [<port_list>] [enable|disable|rx|tx]

7.2.18 Config

Config>	Save <ip_server> <file_name>
	Load <ip_server> <file_name> [check]

7.2.19 SNMP

SNMP>	Trap Inform Retry Times [<retries>]
	Trap Probe Security Engine ID [enable|disable]
	Trap Security Engine ID [<engineid>]
	Trap Security Name [<security_name>]
	Engine ID [<engineid>]
	Community Add <community> [<ip_addr>] [<ip_mask>]

	Community Delete <index>
	Community Lookup [<index>]
	User Add <engineid> <user_name> [MD5|SHA] [<auth_password>] [DES] [<priv_password>]
	User Delete <index>
	User Changekey <engineid> <user_name> <auth_password> [<priv_password>]
	User Lookup [<index>]
	Group Add <security_model> <security_name> <group_name>
	Group Delete <index>
	Group Lookup [<index>]
	View Add <view_name> [included|excluded] <oid_subtree>
	View Delete <index>
	View Lookup [<index>]
	Access Add <group_name> <security_model> <security_level> [<read_view_name>] [<write_view_name>] Access Delete <index>
	Access Lookup [<index>]

7.2.20 Firmware

Firmware>	Load <ip_addr_string> <file_name>

7.2.21 Fault

Fault>	Alarm PortLinkDown [<port_list>] [enable|disable]
	Alarm PowerFailure [pwr1|pwr2|pwr3] [enable|disable]